ICTs AND HUMAN RIGHTS PRACTICE

A REPORT PREPARED FOR THE UN SPECIAL RAPPORTEUR ON EXTRAJUDICIAL, SUMMARY, OR ARBITRARY EXECUTIONS

BY ELLA MCPHERSON

UNIVERSITY OF CAMBRIDGE

CG+HR
CENTRE OF GOVERNANCE AND HUMAN RIGHTS

CENTRE OF GOVERNANCE AND HUMAN RIGHTS

The Centre of Governance and Human Rights (CGHR), launched in 2009, draws together experts, practitioners and policymakers from the University of Cambridge and far beyond to think critically and innovatively about pressing governance and human rights issues throughout the world. The Centre aims to be a world-class interdisciplinary hub for fresh thinking, collaborative research and improving practice.

Since 2011, CGHR has collaborated with the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, providing research support to his mandate. In 2012, a team of researchers produced a 'Research Pack' on the threats to the right to life of journalists for an Expert Meeting held in Cambridge, ultimately contributing to the Special Rapporteur's report that year to the Human Rights Council. In 2013, work began on a broader collaboration studying violations of the right to life across the African continent, culminating in a report, 'Unlawful Killings in Africa,' to guide the Special Rapporteur's future activity.

In 2014, a CGHR research team began a study of how the use of information and communication technologies affects the right to life, resulting in this report and the ICTs and Human Rights blog. This report was originally a discussion document prepared by CGHR Research Associate Dr Ella McPherson in collaboration with the mandate of the Special Rapporteur and ahead of a meeting of experts held in Cambridge in February 2015. The discussion document, as well as the discussion at the expert meeting, contributed to the Special Rapporteur's thematic report on the use of information and communications technologies to secure the right to life, presented at the 29th session of the UN Human Rights Council.

PREFACE BY THE DIRECTOR OF THE CENTRE OF GOVERNANCE AND HUMAN RIGHTS

It gives me great pleasure to see the publication of this important report by CGHR. The Centre has a strong commitment to interdisciplinary research that impacts upon policy and practice, and this report – and the wider engagement with stakeholders that it led to – is exactly the kind of work we pride ourselves in doing well.

Our work with the UN Special Rapporteur on extrajudicial, summary, or arbitrary executions, Professor Christof Heyns, over the past four years represents the Centre's most long-standing initiative in policy-collaboration. The project is linked with an academic partnership with the University of Pretoria, generously supported by the David and Elaine Potter Foundation.

I want to pay particular tribute to the report's author, Dr Ella McPherson, and to Dr Thomas Probert – the two CGHR Research Associates who ran this project. They led a CGHR Research Team including both undergraduates and post-graduate students across three different departments, who made an excellent contribution to the research and created a valuable digital resource for practitioners and researchers working in this field.

This report arises out of a growing interest of the mandate led by Professor Heyns to examine the possibilities of new technology – or new ways of using old technology – to better support the protection of and accountability for the right to life. Given that the norms concerning the right to life have broadly been settled, much of the controversy around the mandate tends to concern facts rather than debates about what should happen. States are not prone to claim the right to kill unlawfully – they rather deny being involved in such practices. This places a premium on questions of fact-finding and evidence, a focus of this report.

The importance of examining the use of Information and Communication Technologies in human rights practice is evident. The relative ease of digital communications provides great affordances to those involved in witnessing, monitoring, and documenting rights abuses. ICTs can support their efforts to advocate, warn, and report to others within and beyond the human rights world, including media and governance actors. Yet these affordances come with risks and challenges. Judging the quality and veracity of information transmitted, managing overwhelming data flows, preventing or reducing vulnerabilities and threats faced by human rights defenders, navigating media wars in which political actors seek to distort public debate to their advantage – these and related concerns take on new and different dimensions in a digital age.

Looking beyond this report and our work for the Special Rapporteur, the Centre of Governance and Human Rights is working on a multitude of issues concerning Human Rights in the Digital Age. One area of particular interest is pluralism, namely how to maintain and foster diversity of perspectives, especially from the least heard, in human rights practice. The same technologies that expand possibilities of communication may lead human rights actors, state and non-state alike, to restrict access to important platforms and spaces of debate and discussion because of the challenges they face. CGHR is well placed to work with policymakers and practitioners to examine this important issue, and others, in the coming years.

Dr Sharath Srinivasan

Director, Centre of Governance and Human Rights
University of Cambridge

EXECUTIVE SUMMARY

The use of information and communication technologies (ICTs) is creating a wealth of new opportunities as well as a variety of new risks for human rights practice. Given the pace of innovation in the development and use of ICTs, our understanding of their impact on human rights lags. This report provides a crucial and in depth look at ICT initiatives and trends across the key human rights practices of prevention, fact-finding, and advocacy, identifying both risks and opportunities.

In prevention, ICTs can be harnessed to protect human rights defenders, to prevent violations in police-civilian interactions, and in data-driven early warning systems and communication-based conflict prevention. That said, ICTs also create new security risks for human rights defenders and can violate the right to privacy.

In fact-finding, ICTs afford the spontaneous and solicited participation of civilian witnesses in the production of human rights evidence. Of course, a greater volume and variety of information from unknown and untrained sources creates problems of misinformation and verification, which technology only goes so far to mitigate.

In advocacy, ICTs provide new channels for quickly and visibly mobilizing publics, for directly engaging with advocacy targets, and for spreading awareness of human rights. That said, the effects of these new advocacy channels are unclear, and they may imperil categories of human rights and the reputations of human rights organizations.

The report also considers how digital divides and the political economy of ICTs influence the nature, extent, and distribution of these opportunities and risks. In doing so, it outlines a research framework for understanding ICTs and human rights practice to underpin academics' and practitioners' assessment, development, and deployment of ICTs for and in the spirit of human rights.

An earlier version of this report, prepared for an expert meeting ahead of the June 2015 session of the UN Human Rights Council, informed the thematic report on ICTs and the right to life presented at that session by the Special Rapporteur on extrajudicial, summary, or arbitrary executions. As such, the projects profiled represent a snapshot of that timeframe; this report is therefore accompanied by a regularly updated, student-run Tumblr blog, ictandhr.tumblr.com, which welcomes submissions on new initiatives.

TABLE OF CONTENTS

ICTs AND HUMAN RIGHTS PRACTICE

A REPORT PREPARED FOR THE UN SPECIAL RAPPORTEUR ON extrajudicial, summary, or arbitrary executions

BY ELLA MCPHERSON

INTRODUCTION[1]

In 2010, the UN Special Rapporteur on extrajudicial, summary, or arbitrary executions, Christof Heyns, received a horrifying video from the UK's Channel 4 that seemed to document the summary execution of Tamil prisoners by Sri Lankan soldiers. This anonymous video, shot on a mobile phone, was an extended version of a video that Heyns' predecessor, Philip Alston, had previously evaluated. If true, the video would be evidence of a grave violation of the right to life – evidence that could not have existed prior to the advent of video-enabled mobile phones.

After receiving the first, shorter version of the video, Alston wrote the Sri Lankan government indicating that the footage warranted an independent investigation. In response, the Sri Lankan government claimed the video had been fabricated, citing analysis it commissioned from audio, video, ballistics, and forensic pathology experts. In turn, Alston also engaged experts, who instead found that the contents of the video indicated authenticity. Heyns gave the extended video to the same experts for review; by examining the footage for indications of editing and the details of the incidents recorded, these experts again concluded that the video depicted real executions. Heyns then reported these findings to the United Nations Human Rights Council, calling on the Sri Lankan Government to investigate the executions.[2]

This pioneering case, which demonstrated both the potential of information and communication technologies (ICTs) for expanding the documentation of human rights violations and the problem of verification this expansion poses, was an impetus for this report.[3] ICTs are unsettling human rights practices across the board, including the key practices of preventing human rights violations, fact-finding cases of violations, and advocating for the amelioration of individual cases as well as for the promotion of a broader culture of human rights.[4] Given the pace of innovation in the development and use of ICTs, our understanding of their impact on human rights often lags. Understanding this impact is crucial not just because of the opportunities ICTs create for human rights – which we can think of as affordances, or

---

[1] I am grateful for insightful comments on the document from Anne Alexander, Richard Danbury, Christof Heyns, Finbarr Livesey, Lucy Purdon, Thomas Probert, Sharath Srinivasan, and the participants in the Expert Meeting. Any errors, of course, remain my own.

[2] Christof Heyns, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns: Addendum*, Human Rights Council 17th Session (United Nations Office of the High Commissioner for Human Rights, 27 May 2011) <www.ohchr.org/Documents/Issues/Executions/A-HRC-17-28-Add1.pdf>.

[3] Given the Special Rapporteur's mandate, the report was originally tailored to human rights work related to the right to life, though much of its content holds for the full array of rights.

[4] Sameer Padania and others, *Cameras Everywhere: Current Challenges and Opportunities at the Intersection of Human Rights, Video and Technology* (Brooklyn, NY: Witness, 2011) <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Witness_1.pdf>.

what ICTs allow their users to do.[5] It is also crucial – due to the 'double-edged' nature of technology – because of the risks.[6]

Information and communication technology is a catchall category that refers to the hardware and software that facilitate the production, storage, transmission, and reception of digital information.[7] The aim of this report, targeted at both practitioners and researchers, is to provide a snapshot of current initiatives and trends at the intersection of ICTs and human rights practices. Based on a review of primary materials documenting these initiatives and trends as well as on interviews with human rights defenders (HRDs), this report examines three key human rights practices in turn.

In prevention, the use of ICTs includes their deployment to protect HRDs, to deter violations through police body-worn cameras, and for conflict prevention and early warning systems. These three uses address hotspots of right to life violations. They also create new security and privacy risks.

In fact-finding, ICTs support both spontaneous and solicited civilian witnessing. ICTs facilitate fact-finders' evaluation of human rights information for evidence – but they also complicate it because of the volume and verification challenges of social media information. Although generating robust evidence is a requirement of all human rights fact-finding, it is particularly relevant for cases involving the violation of the right to life, as one of the major challenges in this area is perpetrators' refutation of allegations of violations.

In terms of advocacy, ICTs provide new opportunities for reaching publics and advocacy targets. Because of social media's particular characteristics and cultures, however, their use may jeopardize the visibility of particular categories of human rights information as well as the reputations of human rights organizations.

Looking at opportunities and risks for human rights practices in the field is key for understanding how using ICTs can impact work to secure the right to life and other human rights. These opportunities and risks are not, however, distributed evenly. Their distribution is inflected by digital divides with respect to access to ICTs as well as with respect to digital literacy, or knowledge about how to use ICTs. These digital divides, as well as the nature of the opportunities and risks that the use of ICTs generates, are in turn influenced by ICTs' political economy, namely the power relations in which the use of particular ICTs are embedded. The conclusion of this report recommends that academics and practitioners take an approach to understanding ICTs and human rights practice that encompasses these aspects as a way to foreground the human rights concerns of redressing power abuses and enabling pluralism in the research, design, and deployment of these ICTs.

---

[5] Jeffrey W. Treem and Paul M. Leonardi, 'Social Media Use in Organizations: Exploring the Affordances of Visibility, Editability, Persistence, and Association', *Communication Yearbook*, 36 (2012), 143–89.

[6] Emma Daly, 'Why Tech Is a Double-Edged Sword for Human Rights', *Human Rights Watch*, 6 January 2014 <www.hrw.org/news/2014/01/06/why-tech-double-edged-sword-human-rights>.

[7] David J. McKenzie, Youth, ICTs, and Development (Washington, DC: World Bank, 2007) <http://documents.worldbank.org/curated/en/2007/03/7458887/youth-icts-development>.

ICTS AND THE HUMAN RIGHTS PRACTICE OF PREVENTION

ICTs support the human rights practice of the prevention of violations in a variety of ways, three of which are addressed here. The first is the physical and digital protection of HRDs. A second category is the deterrence of violations committed by police through the deployment of body-worn cameras. Third are early warning systems and conflict prevention initiatives designed to detect and defuse imminent human rights violations and conflict more broadly.

Of course, these applications all have their risks and shortcomings. For example, the same affordances of digital technology that allow HRDs to alert their networks that they are facing imminent danger – namely geolocation and networked communications – make it easier for those targeting HRDs to identify, surveille, and harass them.[8] Easy documentation with digital video cameras may prevent police abuses, but it may also engender violations of the right to privacy.[9] Though the reach and analytic capabilities of ICTs demonstrate potential for the remote identification of potential human rights hotspots at unprecedented scale and speed, this is not yet translatable into swift action on the ground.[10]

Protection of human rights defenders

Front Line Defenders documented 130 cases of HRDs dying in detention or being killed between January and October of 2014, part of a 'growing global backlash.'[11] HRDs' increasing use of ICTs to communicate, organize, investigate, and advocate facilitates this backlash. For example, HRDs may inadvertently expose their identities and locations – as well as those of their professional and personal networks – or they may unknowingly fall prey to surveillance. This section first overviews a number of the risks for HRDs that are exacerbated by their use of ICTs, and then outlines initiatives to protect them physically as well as digitally.

HRDs' physical security is closely linked to their digital security, and the use of ICTs makes HRDs vulnerable to attacks on both. These attacks are unfortunately part of pattern, and digital attacks in particular build on a history of information wars between HRDs and those seeking retaliation for their work.[12] These digital attacks can be manifested in deception, intimidation, discrediting, censorship, and surveillance. Recent examples include websites that tricked Syrian activists into downloading malware by purporting to provide security tools; the abduction of a

---

[8] Stephanie Hankey and Daniel Ó Clunaigh, 'Rethinking Risk and Security of Human Rights Defenders in the Digital Age', *Journal of Human Rights Practice*, 5 (2013), 535–47 <http://dx.doi.org/10.1093/jhuman/hut023>.

[9] Robert Muggah, 'Why Police Body Cameras Are Taking Off, Even After Eric Garner's Death', *IPI Global Observatory*, 11 December 2014 <http://theglobalobservatory.org/2014/12/police-body-cameras-eric-garner/>.

[10] Sheldon Himelfarb, 'Can Big Data Stop Wars Before They Happen?', *United States Institute of Peace*, 2014 <www.usip.org/publications/can-big-data-stop-wars-they-happen>.

[11] Front Line Defenders, *Front Line Defenders Annual Report 2015: Human Rights Defenders in the Balance* (Front Line Defenders, 13 January 2015) <www.frontlinedefenders.org/2015-Annual-Report>.

[12] Front Line Defenders; Hankey and Clunaigh.

Libyan HRD shortly after he received a threatening message on Facebook; and the UK government's surveillance of Amnesty International's electronic communications.[13]   Across the globe, state censorship and surveillance of the internet have proliferated year on year since Freedom House began tracking it in 2010, and arrests related to internet use are increasing worldwide.[14]

The risks associated with HRDs' use of ICTs are evolving in tandem with the technology. For example, face recognition algorithms are increasingly accurate – and indeed are moving beyond face recognition to matching identities with other idiosyncratic physical characteristics like posture and hairstyle.[15] Results can then be cross-referenced with other data such as Facebook profiles.[16]   The human rights community is often at a disadvantage versus states in the technological 'arms race,' which requires resources like time, money, and expertise. Furthermore, states have a distinct source of leverage over technology companies, in that they can threaten to ban their websites; this leverage may compel companies to hand over user information.[17]

That being said, initiatives are underway to use technology to protect HRDs physically and to equip HRDs to protect themselves digitally. In terms of the former, various organizations are developing alert applications that activists, journalists, and others can use to send a signal that they are in danger. These applications, such as Amnesty International's Panic Button, build on the increasing ubiquity of smartphones. Another example is commercial operator PFO tech's GPS bracelets, developed as part of the Civil Rights Defenders' Natalia Project for human rights practitioners operating in risky situations. Once triggered, the bracelet sends an alarm and position alert to nearby contacts and the headquarters of Civil Rights Defenders, which then sends an alert out to its social media followers. According to

---

[13] Sherif Elsayed-Ali, 'The UK Government Spied on Us and We Won't Take It Lying Down', *Amnesty International*, 2 July 2015 <https://www.amnesty.org/en/latest/news/2015/07/the-uk-government-spied-on-us-and-we-wont-take-it-lying-down/>; John Scott-Railton and Morgan Marquis-Boire, 'A Call to Harm: New Malware Attacks Target the Syrian Opposition', *The Citizen Lab*, 21 June 2013 <https://citizenlab.org/2013/06/a-call-to-harm/>; United Nations Human Rights, 'UN Rights Chief Zeid Condemns Attacks on Human Rights Defenders in Libya', *United Nations Human Rights: Office of the High Commissioner for Human Rights*, 14 October 2014 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15168>.

[14] Sanja Kelly and others, *Tightening the Net: Governments Expand Online Controls* (Freedom House, 2014) <www.freedomhouse.org/report/freedom-net/2014/tightening-net-governments>; Andrew Robertson and Steve Olson, *Sensing and Shaping Emerging Conflicts: Report of a Workshop by the National Academy of Engineering and United States Institute of Peace Roundtable on Technology, Science, and Peacebuilding* (Washington, D.C.: The National Academies Press, 2013) <http://www.usip.org/sites/default/files/Sensing_And_Shaping_Emerging_Conflicts.pdf>.

[15] Aviva Rutkin, 'Facebook Can Recognise You in Photos Even If You're Not Looking', *New Scientist*, 22 June 2015 <https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking>.

[16] Sameer Padania, 'The Ethics of Face Recognition Technology', *WITNESS Blog*, 7 March 2012 <http://blog.witness.org/2012/03/the-ethics-of-face-recognition-technology/>; Natasha Singer, 'Never Forgetting a Face', *The New York Times*, 17 May 2014 <http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html>.

[17] Hankey and Clunaigh; Paul Vale, 'Russia Threatens To Block Facebook, Google And Twitter', *The Huffington Post UK*, 22 May 2015 <http://www.huffingtonpost.co.uk/2015/05/22/russia-threatens-to-ban-facebook-google-and-twitter-unless-companies-turn-over-user-data_n_7423550.html>.

the organization's executive director, the idea is that a HRD wearing the bracelet would have 'millions of people around the world on [her] wrist.'[18]

Technological tools for computer security are increasingly vital to HRDs' safety. These include tools for encryption, namely the mathematical manipulation of information to render it readable solely by the person intended to receive it, and tools for anonymity, the successful concealment of one's identity. As the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion recently reported to the UN Human Rights Council, encryption and anonymity are also vital to our exercise of the human rights within his mandate.[21]

For example, non-profit The Tor Project has developed Tor, communication software that routes data packets through a number of computers, thus disconnecting source and destination.[22] As such, Tor facilitates anonymity, which affords the formation of opinion by allowing users to freely search and research online.[23] Detekt, developed via a partnership between Amnesty International, Digitale Gesellschaft, Electronic Frontier Foundation and Privacy International, allows individuals to scan their computers for spyware designed to circumnavigate encryption.[24]

> **Amnesty International's Panic Button**
>
> *The Panic Button app allows users to secretly activate SMS messages containing an alarm message and, optionally, geolocation data. These messages are sent to three pre-selected peers through rapidly pressing the mobile phone's power button. When HRDs or journalists are attacked or arrested, they are usually forced to relinquish their phones for the lists of contacts they store. As long as Panic Button, which is disguised as a mundane app, is not discovered on the phone, and as long as the phone is still on and within range, it will continue to broadcast alerts. These alerts are not only calls for help but also indicate to recipients that they should take security precautions themselves. Activists testing the Panic Button app have reported that the process has prompted them to strengthen their overall security plans.[19] Amnesty developed the Panic Button Android app in collaboration with iilab, the engine room, and Front Line Defenders; funders include the Ford Foundation and Google.[20]*

Just because these physical and digital security tools exist, however, does not mean they are at HRDs' fingertips.[25] First of all, governments are enacting or considering

---

[18] Nina Strochlic, 'Can This Bracelet Save Your Life', *PFO Tech*, n.d. <http://www.pfotech.com/2013/04/06/can-bracelet-save-life-newsweek/>.

[19] Tanya O'Carroll, 'More than an App: The Panic Button, One Year on', *Amnesty International*, 22 July 2015 <https://www.amnesty.org/en/latest/campaigns/2015/07/panic-button-one-year-on/>.

[20] Tom Watson, 'Inside Amnesty's Panic Button App: Simple Technology, Serious Impact For Activists', *Forbes*, 23 June 2014 <http://www.forbes.com/sites/tomwatson/2014/06/23/inside-amnestys-panic-button-app-simple-technology-serious-impact-for-activists/>.

[21] David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, Human Rights Council 29th Session (United Nations Office of the High Commissioner for Human Rights, 22 May 2015) <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>.

[22] Tor, 'Tor: Overview', *Tor*, n.d. <https://www.torproject.org/about/overview.html.en>.

[23] Kaye.

[24] Detekt, 'Intentions and Methods', *Detekt: Resist Surveillance*, n.d. <https://resistsurveillance.org/intentions.html>.

limits to online encryption and anonymity. For example, South Korea requires users to register with their real names when they access certain online spaces.[26] In Ethiopia, a number of bloggers who wrote about human rights were arrested for treason, and their use of Security-in-a-Box, a digital security resource, was presented as evidence against them.[27] The UK government has recently revived arguments for backdoors built into encryption to allow the government to read communications encrypted by that technology. This argument has resurfaced despite security experts' assertion that these backdoors are operationally and technically infeasible.[28]

Second, as the famous experiment titled, 'Why Johnny Can't Encrypt,' demonstrates, a gap can exist between the language of programmers creating these tools and the literacy of users. Two-thirds of this experiment's relatively well-educated test subjects could not ascertain how to encrypt and sign an email using PGP 5.0, even though they had full access to the PGP manual and ninety minutes to try.[29] Digital literacy, as a new element of the human rights toolkit, presents a steep learning curve, and HRDs are often already very pressed for time and resources.[30] This lack of digital literacy on security is a problem across the board for HRDs, from NGOs to the UN Human Rights Council, where, for example, several mechanisms solicit reports of human rights violations over email without indicating attendant risks or strategies for more secure communications.[31]

ICTs for physical and digital security can be useless or even dangerous without adequate training. For example, personal security apps may embolden human rights practitioners to take excessive risks if they do not anticipate that these apps only work in areas with mobile coverage and plan accordingly.[32] As Neu writes, 'Sooner

---

[25] For more on these themes, see the summary of a recent workshop co-hosted by CGHR and Amnesty International: Rebekah Larsen and Ella McPherson, 'Encryption, Anonymity & Human Rights Workshop', *Centre of Governance and Human Rights, University of Cambridge*, 2015 <http://www.cghr.polis.cam.ac.uk/research-themes/human-rights-in-the-digital-age-1/encryption-and-human-rights-workshop>.

[26] Anna Crowe, Sarah Lee and Mark Verstraete, *Securing Safe Spaces Online: Encryption, Anonymity, and Human Rights* (Privacy International, 2015) <https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf>.

[27] Front Line Defenders.

[28] Harold Abelson and others, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report, 6 July 2015 <http://www.cl.cam.ac.uk/~rja14/Papers/doormats.pdf>.

[29] Alma Whitten and J. D. Tygar, 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0', in *Security and Usability: Designing Secure Systems That People Can Use*, ed. by Lorrie Cranor and Garfinkel Simson (Sebastopol, CA: O'Reilly Media, Inc., 2005), pp. 679–702.

[30] Hankey and Clunaigh.

[31] Christof Heyns, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns: Use of Information and Communications Technologies to Secure the Right to Life*, Human Rights Council 29th Session (United Nations Office of the High Commissioner for Human Rights, 24 April 2015) <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>.

[32] Cynthia Romero, *What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World* (USAID, 2014) <https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf>.

or later, all technology problems become education problems.'[33]   Consequently, a number of online digital literacy resources targeted at HRDs exist. These include the aforementioned Security-in-a-Box, developed by the Tactical Technology Collective and Front Line Defenders, as well as the digital security helpline provided by Access, an NGO focused on digital rights.[34]   Another NGO, New Tactics in Human Rights, creates spaces for online knowledge exchange between HRDs on aspects of human rights practice, including digital security.[35]

Developers and trainers tend to caution users not to ever expect full privacy and anonymity online. Panic Button, for example, warns, 'It is important to start with the understanding that mobile phones are inherently insecure,' both in their storage and transmission of information and because smartphones, by default, share information about their usage and locations.[36] This risk has impelled some HRDs to conduct their work entirely offline.   Others are highly public about their identities and their activities online, based on the belief that publicity can provide protection. Some activists in China, for example, reported pretending to film after their phones ran out of batteries as a shield against abduction or arrest.[37] This use of technology, where digital documentation is an intended deterrent, also underpins the use of police body-worn cameras.

Police body-worn cameras

Calls for greater police accountability have amplified in the wake of several recent police shootings in the United States, including the killing of teenager Michael Brown in Ferguson, Missouri. The number of individuals killed by law enforcement in the U.S. is unknown, as the government does not collect this figure. Annual estimates range from approximately 400 'justifiable police homicides,' as reported by police officers, to between 600 and 1,000, as estimated by journalists and civilian investigators.[38] A high salience idea in current debates about police violence – and the subject of a recent $236m investment by the U.S. government – is the police use of wearable technology in the form of body-worn cameras.[39] This idea operates on the assumption that filming police interactions with civilians will check abuses as well as provide evidence should accusations of misconduct be levied against either

---

[33] Christopher Neu, 'Mobile Applications for Atrocity Prevention Require Mobile Students', *TechChange*, 2013 <http://techchange.org/2013/02/19/mobile-applications-for-atrocity-prevention-require-mobile-students/>.

[34] Access, 'Access Tech', *Access* <https://www.accessnow.org/pages/tech#Digital%20Security%20Helpline>.

[35] New Tactics in Human Rights, 'Staying Safe: Security Resources for Human Rights Defenders', *New Tactics in Human Rights*, 2010 <https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders>.

[36] Panic Button, 'Managing Your Risks', *Panic Button*, n.d. <https://panicbutton.io/help/help-risk.html>.

[37] Hankey and Clunaigh.

[38] Annie Waldman, 'Death by Cop: Invisible Numbers', *BBC News*, 27 August 2014 <http://www.bbc.co.uk/news/blogs-echochambers-28946204>.

[39] Muggah.

police or civilians.[40] Indeed, a study of police in Rialto, California found that officers' use of force dropped by 59% upon the introduction of body-worn cameras.[41]

> ### *CopCast*
>
> *A cornerstone of the Igarapé Institute's Smart Policing programme is CopCast, open-source software that allows smartphones to be used as body-worn cameras transmitting video, audio, and geolocation coordinates from officers on patrol back to headquarters.[42] Police are currently testing it in Rio de Janeiro, Brazil; Nairobi, Kenya; and Cape Town, South Africa.[43] Igarapé is developing the programme in partnership with the African Policing and Civilian Oversight Forum and with support from Google.*

The institutionalization of these cameras may be an even greater deterrent of abuses than smartphone-enabled civilian witnessing of incidents, such as the 2014 death of Eric Garner following a chokehold by a New York City Police Department officer and filmed by a bystander. This is because institutionalized use, which requires police to warn civilians that they are recording, creates 'cognition of surveillance' among both police and civilians, potentially moderating behaviour.[44]

Police around the world, including the New York City Police Department, the Jamaica Constabulary Force, and the London Metropolitan Police, are trialling versions of police body-worn cameras. A police department in the U.S. state of Georgia, for example, uses Google Glass to record interactions with civilians, and the recordings are transmitted real-time back to the police station for monitoring.[45] In another example, the police in Calgary, Canada, plan to layer on face-recognition software to analyse the footage collected by their cameras.[46]

As much as these programmes are generating interest, they are also generating concerns, particularly around possible violations of the right to privacy. Some have suggested that the cameras be turned off upon entering a home or when speaking with survivors of sexual assaults and minors. Given the potentially sensitive nature of this footage, access to information and the security of its storage must be a consideration.[47] A separate concern is selective documentation; a suggested remedy

---

[40] Josh Sanburn, 'Police Eye Google Glass as Surveillance Tool', *Time*, 17 February 2014 <http://nation.time.com/2014/02/17/police-eye-google-glass-as-surveillance-tool/>.

[41] Fred Lewsey, 'First Scientific Report Shows Police Body-Worn-Cameras Can Prevent Unacceptable Use-of-Force', *University of Cambridge*, 23 December 2014 <http://www.cam.ac.uk/research/news/first-scientific-report-shows-police-body-worn-cameras-can-prevent-unacceptable-use-of-force>.

[42] Amar Toor, 'Camera Cops: Digital Spying in Rio's Most Dangerous Slums', *The Verge*, 21 October 2013 <http://www.theverge.com/2013/10/21/4861176/smart-policing-android-app-igarape-google-ideas-police-surveillance-rio-favelas>.

[43] Igarapé Institute, 'Smart Policing', *Igarapé Institute: Progressive Alternatives for Security and Development*, n.d. <en.igarape.org.br/smart-policing/>.

[44] Lewsey.

[45] Sanburn.

[46] BBC News, 'Met Officers to Trial Body Cameras', *BBC News London*, 8 May 2014 <www.bbc.co.uk/news/uk-england-london-27313500>; John Lorinc, 'New Era of Policing: Will the Benefits of Body-Worn Cameras Outweigh the Privacy Issues?', *The Globe and Mail*, 21 November 2014 <http://www.theglobeandmail.com/news/national/new-era-of-policing-will-the-benefits-of-body-worn-cameras-outweigh-the-privacy-issues/article21698547/>; Alphea Saunders, 'Body Cameras for Policemen', *Jamaica Information Service*, 2014 <http://jis.gov.jm/body-cameras-policemen/>.

[47] Bracken Stockley, 'Public Support for Police Body Cameras – but Who Controls On/off Switch?', *The Justice Gap*, 2014 <http://thejusticegap.com/2014/03/body-worn-video-cameras-scrutiny/>.

is stipulating that individual police officers have no control over when the camera is filming or how footage is edited.[48] Another remedy, being promoted in particular by activists in the U.S., is raising awareness of civilians' right to record back.[49] Despite these limitations, the hope is that police body-worn cameras can serve as a conflict prevention mechanism.

Conflict prevention and early warning systems

Actors are deploying ICTs for prevention through mitigation and through prediction in hotspots of potential human rights violations and broader conflict. Examples of conflict prevention rest on ICTs' communication affordances. Tactics include the diffusion of peace-promoting messages, as with PeaceTXT in Kenya, and the screening of communications for hate speech, as mobile network operator Safaricom did during the 2013 Kenyan election.[50] Another approach is livestreaming situations that threaten individuals' human rights as they unfold. This 'co-presence for good' relies on livestreaming video apps, such as Twitter's Periscope, in combination with smartphones or wearable cameras such as Google Glass and potentially also with virtual reality technology so that audiences can experience 'being there' in real-time.[51] These audiences can include experts, such as lawyers, conducting live analysis of the situation and feeding it back to the person on the ground.[52] In a sense, co-presence collapses the categories of prevention, fact-finding, and advocacy. Knowledge of the co-presence of others may stymie violations, while these others are witnesses and a natural advocacy group if a violation does take place. Of course, co-presence also creates risks due, for example, to the impossibility of editing out subjects who request anonymity or are in danger.[53]

The affordances of ICTs for the rapid and widespread collection, analysis, and communication of information undergird early warning systems. Aymta, an early warning system for scud missiles in Syria, was one such example – though it is now defunct in part due to a lack of funding, a common problem for 'peacetech'

---

[48] Sanburn.

[49] Nadia Kayyali, 'Want to Record The Cops? Know Your Rights', *Electronic Frontier Foundation*, 2015 <https://www.eff.org/deeplinks/2015/04/want-record-cops-know-your-rights>.

[50] Sonni Efron, 'Meet the Hacktivist Who Wants to Warn Syrians About Incoming Missiles', *The Atlantic*, 2 July 2013 <www.theatlantic.com/international/archive/2013/07/meet-the-hacktivist-who-wants-to-warn-syrians-about-incoming-missiles/277461/>; Sheldon Himelfarb and Anand Varghese, 'Peace, Inc.', *Foreign Policy*, 2015 <foreignpolicy.com/2015/01/27/peace-inc-tech-government-industry-defense-funding/>; Patrick Meier, 'PeaceTXT Kenya: Since Wars Begin in the Minds of Men', *PopTech*, 4 March 2013 <http://poptech.org/blog/peacetxt_kenya_since_wars_begin_in_the_minds_of_men>; Lucy Purdon, *Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections, Case Study: Safaricom* (Institute for Human Rights and Business, 2013) <http://www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf>.

[51] Sam Gregory, 'How We Can Use Livestreaming Apps to Promote Justice', *WIRED*, 10 May 2015 <www.wired.com/2015/05/can-use-livestreaming-apps-promote-justice/>.

[52] Sam Gregory, 'Co-Presence: A New Way to Bring People Together for Human Rights Activism', *WITNESS Blog*, 23 September 2013 <blog.witness.org/2013/09/co-presence-for-human-rights/>.

[53] Sam Gregory, 'How We Can Use Livestreaming Apps to Promote Justice', *WIRED*, 2015 <http://www.wired.com/2015/05/can-use-livestreaming-apps-promote-justice/> [accessed 13 May 2015].

entrepreneurs.[54]   Other initiatives analyze real-time or near real-time big data with an aim to forecasting escalating violence. Hatebase, for example, developed by The Sentinel Project and Mobiocracy, monitors the vocabulary and incidence of hate speech – which is correlated with a risk of genocide – on social media.[55]   Satellite monitoring projects, such as the Satellite Sentinel Project, aim to detect potential violations, as well as to deter and document them.[56]   Speculation also exists about the increasing use of drones for the same purposes of remote sensing.[57]

In practice, however, significant limitations exist to the possibilities of ICTs for early warning systems.   First of all, some initiatives – such as human rights monitoring via drones – raise questions about surveillance and privacy.[60] Second, early warning systems based on big data mining are

The Satellite Sentinel Project

The Satellite Sentinel Project stems from a partnership between the Enough Project of the Center for American Progress and remote sensing company DigitalGlobe, as well as previous collaborations with the United Nations UNITAR Operational Satellite Applications Programme (UNOSAT) and the Harvard Humanitarian Initiative, among others. It monitors the border between Sudan and South Sudan for actual and potential threats against civilians. As with the police body-worn cameras initiatives, the project assumes that satellite monitoring may deter. Raising awareness among potential perpetrators that vulnerable areas are being watched could stymie violations – at least the kinds that are visible remotely.[58] Celebrity co-founder George Clooney likened this to a paparazzi effect with anti-genocide aims, saying, 'We want them to enjoy the level of celebrity attention that I usually get. If you know your actions are going to be covered, you tend to behave much differently than when you operate in a vacuum.'[59]

imbalanced with respect to providing the full suite of functions necessary for a successful intervention.   We can understand the latter as depending on the execution of three stages: information collection, information analysis, and information transmission to local and international actors.[61]   Though current initiatives are strong on data collection, they are weaker on analysis and actionable

---

[54] Ciara Byrne, 'Welcome To PeaceTech, The Movement To Use Technology To End Violent Conflict And Extremism', *Fast Company*, 11 August 2015 <http://www.fastcoexist.com/3047534/welcome-to-peacetech-the-movement-to-use-technology-to-end-violent-conflict-and-extremism>.

[55] Timothy Quinn, 'Introducing Hatebase: The World's Largest Online Database of Hate Speech', *The Sentinel Project*, 2013 <https://thesentinelproject.org/2013/03/25/introducing-hatebase-the-worlds-largest-online-database-of-hate-speech/>; Timothy Quinn, 'Meet HateBrain, the Automated Social Media Monitoring Engine at the Heart of Hatebase', *The Sentinel Project*, 2013 <https://thesentinelproject.org/2013/07/23/meet-hatebrain-the-automated-social-media-monitoring-engine-at-the-heart-of-hatebase/>.

[56] Ben Yunmo Wang and others, 'Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities', *Stability: International Journal of Security & Development*, 2 (2013), 53 <http://dx.doi.org/10.5334/sta.cn>.

[57] Andrew Stobo Sniderman and Mark Hanis, 'Drones for Human Rights', *The New York Times*, 30 January 2012 <www.nytimes.com/2012/01/31/opinion/drones-for-human-rights.html>.

[58] Nathaniel A. Raymond and others, 'While We Watched: Assessing the Impact of the Satellite Sentinel Project', *Georgetown Journal of International Affairs*, 26 July 2013 <http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/>.

[59] Patrick Meier, 'Will Using "Live" Satellite Imagery to Prevent War in the Sudan Actually Work?', *iRevolutions*, 30 December 2010 <http://irevolution.net/2010/12/30/sat-sentinel-project/>.

[60] Sarah Stein Kerr, 'Drones for Good? The Basic Human Rights Considerations', *WITNESS Blog*, November 2013 <https://blog.witness.org/2013/11/drones-for-good-the-basic-human-rights-considerations/>.

[61] Robertson and Olson.

transmission.[62]   Questions also arise as to the effectiveness of monitoring for deterrence if this monitoring is not coupled with the credible threat of punitive measures.[63]

The use of big data and remote sensing for the prevention of human rights violations also raises methodological and ethical concerns. The Human Rights Data Analysis Group highlights sources of potential inaccuracies in the statistical analysis of human rights data arising from selection bias, duplication, and constraints on data capture.[64] Others caution that the increasing quantification of human rights practice may abstract human rights violations, distract from the discussion about accountability with a conversation about technicalities, and obscure the politics in which the processes of counting and using numbers are embedded.[65] Some warn that the lack of a coherent ethical framework around the use of remote sensing data in human rights practice may result in situations where vulnerable populations are put at risk through the remote documentation of their locations and situations.[66]   In consideration of these concerns, the Harvard Humanitarian Initiative has launched The Signal Program on Human Security and Technology to develop strategies and ethical guidelines around the use of remote sensing in human rights and humanitarian work.[67] In sum, the use of ICTs hold promise for the prevention of human rights violations, but only if informed by an understanding of how these opportunities and their attendant risks and limitations intersect with the contexts of their deployment.

---

[62] Himelfarb.

[63] Meier, 'Will Using "Live" Satellite Imagery to Prevent War in the Sudan Actually Work?'.

[64] Human Rights Data Analysis Group, 'Core Concepts', *Human Rights Data Analysis Group*, 2015 <hrdag.org/coreconcepts/>.

[65] Kelly M. Greenhill, 'Nigeria's Countless Casualties: The Politics of Counting Boko Haram's Victims', *Foreign Affairs*, 9 February 2015 <www.foreignaffairs.com/articles/africa/2015-02-09/nigerias-countless-casualties>; Margaret L. Satterthwaite and Justin Simeone, *An Emerging Fact-Finding Discipline? A Conceptual Roadmap for Social Science Methods in Human Rights Advocacy*, Public Law & Legal Theory Research Paper Series (New York, NY: New York University School of Law, 2014) <http://papers.ssrn.com/abstract=2468261>.

[66] Robertson and Olson.

[67] Harvard Humanitarian Inititative, 'The Signal Program on Human Security and Technology', *Harvard Humanitarian Initiative*, 2013 <hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program>.

ICTS AND THE HUMAN RIGHTS PRACTICE OF FACT-FINDING

Like prevention, holding perpetrators to account for human rights violations is core to the work of the human rights community. This involves the gathering and evaluation of information for evidence – namely the practices of fact-finding addressed in this section – followed by advocacy based on that evidence, addressed in the next section.[68] The evidence may also – or alternatively – be destined for court, in which case it will have to meet specific criteria for admissibility; the evidence that can be used to generate denunciation through advocacy cannot necessarily be used for justice in the courts.[69]

Human rights organizations have developed rigorous fact-finding methodologies to protect the credibility of their evidence and thus its effectiveness in advocacy and courts. The credibility of the evidence they deploy is also important for human rights organizations' overall reputations of credibility. This reputational resource is key to human rights organizations' persuasiveness in the context of the counter-claims and discrediting discourses that are often among the reactions to their work.[70]

Consequently, the human rights community has developed methodological expertise in evaluating information for evidence, part of the professionalization of human rights over three generations of actors and tactics.[71] Intergovernmental organizations drove the first generation of fact-finding, in which diplomats, experts, and lawyers reviewed on-the-ground research to write reports for governments and intergovernmental groups. Large, international human rights NGOs spearheaded the second generation, which drew largely on witness interviews and produced reports targeted at public opinion and political bodies. The third generation is born of ICTs and a growing number and diversity of players in the human rights fact-finding arena. This current generation is characterised by the replacement of previous 'one-

---

[68] Ann Marie Clark, *Diplomacy of Conscience: Amnesty International and Changing Human Rights Norms* (Princeton, NJ: Princeton University Press, 2001).

[69] Madeleine Bair, 'When YouTube Videos Expose Crimes That Go Unpunished', *PBS Mediashift*, 24 February 2014 <http://www.pbs.org/mediashift/2014/02/when-youtube-videos-expose-crimes-that-go-unpunished/>; Satterthwaite and Simeone.

[70] Amnesty International, 'Legal and Research Tools', *Amnesty International*, 2015 <www.amnesty.org/en/human-rights-defenders/resources/legal-and-research-tools>; L. David Brown, *Creating Credibility* (Sterling, VA: Kumarian Press, Inc., 2008); Alison Brysk, *The Politics of Human Rights in Argentina: Protest, Change, and Democratization* (Stanford, CA: Stanford University Press, 1994); Margaret Gibelman and Sheldon R. Gelman, 'A Loss of Credibility: Patterns of Wrongdoing Among Nongovernmental Organizations', *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, 15 (2004), 355–81 <http://dx.doi.org/10.1007/s11266-004-1237-7>; Molly Land, 'Networked Activism', *Harvard Human Rights Journal*, 22 (2009), 205–43; Molly Land, 'Peer Producing Human Rights', *Alberta Law Review*, 46 (2009), 1115–39; Ella McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models', *American Behavioral Scientist*, 59 (2014), 124–48 <http://dx.doi.org/10.1177/0002764214540508>; Steven R. Ratner, 'The Political Dimension of International Human Rights Fact-Finding', in *Proceedings of the Annual Meeting (American Society of International Law)*, 2013, CVII, 70–72; Margaret Satterthwaite, 'Finding, Verifying, and Curating Human Rights Facts', in *Proceedings of the Annual Meeting (American Society of International Law)*, 2013, CVII, 62–65.

[71] Philip Alston, 'Introduction: Third Generation Human Rights Fact-Finding', in *Proceedings of the Annual Meeting (American Society of International Law)*, 2013, CVII, 61–62; Land, 'Peer Producing Human Rights'.

size-fits-all' models with more flexibility in fact-finding methodology and research output.[72] As Satterthwaite explains it:

> Human rights researchers are no longer expected only to 'find' and report on facts; now, they are also expected to create facts through quantitative and statistical analysis; to verify facts established through crowd-sourcing, social media, and citizen journalism; and to curate facts through new forms of visual display, including through web-based photojournalism or documentaries and the use of visual analytical tools such as sophisticated – and often interactive – data visualization.[73]

It is the impact of ICTs on this third generation of fact-finding that is of concern here. A major change, building on ICTs' affordance of user-generated content, has been the escalation of information produced and transmitted by civilian witnesses, whether spontaneous or solicited.[74] These new channels and sources of information introduce various challenges, including: (1) the security challenge for the contents, subjects, and witnesses of reports; (2) the volume challenge, namely the risk that evidence is lost in the deluge of digitally-enabled civilian witness information that takes time and expertise to parse; and (3) the verification challenge, related to the risk of misinformation arising from ICTs' facilitation of information production, transmission, and manipulation. This section first outlines the nature and challenges of spontaneous and solicited digital civilian witness information. It goes on to explore technologies and tactics deployed against these challenges of ICTs for the practice of human rights fact-finding.

Digital human rights reporting by civilian witnesses

The contributions of ICTs to the third generation of human rights fact-finding centres on their facilitation of civilian witnessing of human rights violations. Through the definition of a civilian as outside of the profession in question, this nomenclature highlights the inexpert nature of the production of information by civilian witnesses.[75] Information from civilian witnesses has long been a cornerstone of human rights fact-finding, in part because of the human rights community's commitment to amplifying the voices of those challenging the powerful, such as state actors.[76] Traditionally, this information tended to be gathered by human rights fact-finders.

---

[72] Alston, CVII, p. 61.

[73] Satterthwaite, CVII, p. 65.

[74] McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'.

[75] Ella McPherson, 'Digital Human Rights Reporting by Civilian Witnesses: Surmounting the Verification Barrier', in *Produsing Theory in a Digital World 2.0: The Intersection of Audiences and Production in Contemporary Theory*, ed. by Rebecca Ann Lind (New York, NY: Peter Lang Publishing, 2015), II, 193–209.

[76] Satterthwaite, CVII; Satterthwaite and Simeone.

What ICTs introduce, however, is the ability of civilian witnesses to autonomously produce and transmit information, facilitated by technologies such as smartphones and social media applications. Of course, it is not just witnesses and subjects of violations that are producing this information, but also perpetrators. Furthermore, the production of this information and its use as evidence do not necessarily mean it is shared publicly, nor does sharing it publicly indicate an intention for it to be used as evidence.[77] As a whole, this information is characterised by its step-change in volume as well as the extent to which the process of producing it is outside of the control of human rights fact-finders – even in instances where human rights fact-finders solicit information via digital channels, such as in crowdsourcing and crowdseeding. In other words, ICTs afford the rise of amateurs in a fact-finding process traditionally dominated by professionals.[78]

Civilian witnessing is, at first glance, a boon, especially in closed-country contexts like Syria. Consider, for example, the fact that local reports about the Syrian government's 2013 chemical weapons attack in Ghouta appeared on social media within hours of the attack.[79] In contrast, the regime of the current president's father was able to keep the details of the 1982 Hama massacre under wraps for quite some time.[80]

Additional benefits include increasing the capacity of human rights fact-finding by harnessing civilian witnesses' spare time, energy, and expertise.[81] Consulting civilian witnesses can also tap into areas of knowledge – particularly knowledge of local contexts – that are unfamiliar to human rights fact-finders based elsewhere. Furthermore, involving civilian witnesses can fire up public enthusiasm about human rights and strengthen the effects of human rights advocacy through greater participation in and awareness of human rights investigations.[82] This section overviews various digital ICT initiatives that facilitate civilian witnesses' production and transmission of information, looking first at spontaneous civilian witnessing and then at information solicited via crowdsourcing and crowdseeding.

Spontaneous reports from civilian witnesses

Civilian witnesses' production and transmission of information, at its most spontaneous, can occur through pre-existing hardware and software without any particular expertise on the part of witnesses. The growing ubiquity of smartphones affords the easy capture of visual and auditory information, and this information can be quickly transmitted through digital channels such as social media – to the extent

---

[77] Christoph Koettl, 'About & FAQ', *Citizen Evidence Lab*, 2014 <www.citizenevidence.org/about/>.

[78] Land, 'Peer Producing Human Rights'.

[79] Office of the Press Secretary, 'Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013', *The White House*, 2013 <http://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21>.

[80] Marc Lynch, Deen Freelon and Sean Aday, *Syria's Socially Mediated Civil War* (Washington, D.C.: United States Institute of Peace, 13 January 2014) <http://www.usip.org/publications/syria-s-socially-mediated-civil-war>.

[81] Land, 'Peer Producing Human Rights'.

[82] Land, 'Peer Producing Human Rights'.

that the conflict in Syria has been referred to as the 'YouTube War.'[83]   That being said, these mainstream digital tools also present a number of challenges for civilian witnessing.

A major challenge is security; mainstream social media applications can risk the security of the information, its subjects, and its civilian witness sources.   The information is in peril because human rights content of a graphic nature runs the risk of being deleted from social media for contravening permissible content policies. Subjects may be identified by their adversaries and may be re-victimized through public exposure.[84]   Civilian witnesses can put themselves in danger both in the production and in the transmission of information.

A second challenge is the quantity of social media information, whether relevant to the incident in question or not.   Some contemporary conflicts have a 'big data problem' (of course, some have the opposite problem because of digital divides in terms of access to and familiarity with technology).[85]   This means that identifying relevant information is like searching for a needle in a haystack.   As Morgan of CrisisNET describes it:

> …Assessing a conflict like the Syrian civil war using social media is the equivalent of aimlessly wandering around Damascus, hoping to stumble upon an interesting discussion. There are tens of thousands of disparate, sometimes enlightening, but often frivolous conversations at any given moment, and the sheer volume of information can be overwhelming.[86]

A third challenge is the quality of the information as regards the ease of verification. Social media information is often characterised by unknown sources and a paucity of metadata.   Metadata is information about the information in question – such as source, place, and time of production.   It is fundamental to the verification process, which hinges on the cross-corroboration of information's content and metadata using other methods and sources.   Mainstream social media applications do not usually prompt users to enter metadata; furthermore, they often strip out metadata generated by standard photo and video applications at the point of upload.[87]   ICTs also facilitate the spread of manipulated information, as evident in 2014's 'SYRIA! SYRIAN HERO BOY rescue girl in shootout' viral video, revealed to be a cinematic

---

[83] Christoph Koettl, '"The YouTube War": Citizen Videos Revolutionize Human Rights Monitoring in Syria', *PBS*, 18 February 2014 <www.pbs.org/mediashift/2014/02/the-youtube-war-citizen-videos-revolutionize-human-rights-monitoring-in-syria/>.

[84] Madeleine Bair, 'Navigating the Ethics of Citizen Video: The Case of a Sexual Assault in Egypt', *Arab Media & Society*, 19 (2014), 1–7; Sam Gregory, 'Images of Horror: Whose Roles and What Responsibilities?', *WITNESS Blog*, 18 September 2014 <blog.witness.org/2014/09/sharing-images-horror-roles-responsibilities/>.

[85] Lara Setrakian, 'Citizen Video for Journalists: Contextualization', *WITNESS Blog*, 1 April 2013 <http://blog.witness.org/2013/04/citizen-video-for-journalists-contextualization/>.

[86] Jonathon Morgan, 'Syrian Social Media, Journalists' Secret Weapon in the Crisis Data Revolution', *CrisisNET*, 3 June 2014 <http://blog.crisis.net/syrian-social-media-journalists-secret-weapon-in-the-crisis-data-revolution/>.

[87] Mike Ashenfelder, 'Social Media Networks Stripping Data from Your Digital Photos', *The Signal: Digital Preservation, Library of Congress Blog*, 2013 <blogs.loc.gov/digitalpreservation/2013/04/social-media-networks-stripping-data-from-your-digital-photos/>.

production disguised as a civilian witness account. Of course, this is also evident in more nefarious attempts to disseminate falsehoods via social media.[88]

Solicited reports from civilian witnesses: crowdsourcing and crowdseeding

Somewhere between human rights fact-finders' traditional methods of gathering information and civilian witnesses' digitally-enabled spontaneous production and transmission are the practices of crowdsourcing and crowdseeding. Crowdsourcing involves institutions turning over tasks normally done by a specific individual to a big, unspecified group recruited through an open call.[89] In this case, professional human rights fact-finders are experimenting with relinquishing the production of information to the crowds of civilian witnesses, often by deploying crowdsourcing tools such as those developed by Ushahidi.

Crowdseeding was born in part out of the concern that crowdsourcing is not exactly representative, but rather tends to attract participants with technology, money, and time – in other words, it attracts the relatively well-resourced.[92] As showcased by the Voix des Kivus project in the Democratic Republic of the Congo, crowdseeding is a category of bounded crowdsourcing.[93] Participants can be randomly sampled for representativeness and equipped with the technology and resources necessary to produce and transmit the information being sought. A relationship develops over time between chosen civilian witnesses and the project, engendering credibility and trust that

> ### Ushahidi and Syria Tracker
>
> Ushahidi, Swahili for 'testimony,' is a non-profit company that, among other services, provides open source reporting and mapping tools. It was founded during the 2008 post-election violence in Kenya and initially aimed to plot crowd-sourced reports of violence and conflict resolution. Ushahidi built on that experience to develop crowdsourcing tools that anyone can adopt.[90]
>
> In 2011, Humanitarian Tracker adopted Ushahidi to power Syria Tracker. Its team, made up of activists in Syria and the U.S., maps reports related to the conflict, such as deaths, detentions, chemical poisonings, and rape. These reports include information extracted using data-mining from more than 80 million social media posts and 160,000 media reports, as well as more than 4,000 eyewitness reports. The latter incorporates crowdsourced information submitted via the project's website as well as information from more than 600 amateur reporters on the ground in Syria. Before making reports public, the team verifies them via corroboration of time and place with other reports, which means that published reports make up only 6% of all the reports collected by Syria Tracker.[91]

---

[88] Madeleine Bair, 'Will the Syrian Hero Boy Make Us Question Everything We See? (and Why Don't We Do That Already?)', *WITNESS Blog*, 20 November 2014 <http://blog.witness.org/2014/11/syrian-hero-boy/>.

[89] Jeff Howe, 'Crowdsourcing: A Definition', *Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*, 2006 <crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html>.

[90] Ushahidi, 'Ushahidi's Mission', *Ushahidi*, 2015 <http://www.ushahidi.com/mission/>.

[91] Vicky Baker, 'Syria's Inside Track: Mapping Citizen Reporting', *Index on Censorship*, 43 (2014), 93–95 <http://dx.doi.org/10.1177/0306422014535688>.

[92] Patrick Meier, 'From Crowdsourcing Crisis Information to Crowdseeding Conflict Zones (Updated)', *iRevolutions*, 10 July 2012 <http://irevolution.net/2012/07/10/crowdsourcing-to-crowdseeding/>.

[93] Peter van der Windt, 'Voix Des Kivus: A Crowd-Seeding System in DRC', *Ushahidi*, 16 May 2011 <http://www.ushahidi.com/blog/2011/05/16/voix-des-kivus-a-crowd-seeding-system-in-drc/>.

facilitate communication.[94]

Like spontaneous civilian witnessing, solicited civilian witnessing creates new challenges. Solicited reports may be submitted privately, which does mitigate some of the security risks of spontaneous public reports over social media. But other risks may stem from crowdsourcing and crowdseeding projects' tendency to publicly map information, which – like satellite images – may jeopardise vulnerable populations in those terrains.[95] Another susceptibility is uncertainty around who exactly is soliciting the reports, and to what end. For example, a malevolent regime might deploy Amazon's Mechanical Turk, a brokerage service providing micro-task labourers, to match faces from photographs of protests with photographs from national identity cards – perhaps even disguised as a game.[96] The volume and verification challenges of solicited information are perhaps not as extensive as those of spontaneous information, since crowdsourcing and crowdseeding projects solicit on-topic information and can prompt witnesses to include metadata. That being said, these challenges remain a concern in human rights fact-finders' evaluation of digital civilian witness information for evidence.

Fact-finders' evaluation of civilian witness information for evidence

The digital flood of information from civilian witnesses only has evidentiary potential if human rights fact-finders successfully evaluate it. The evaluation of information for evidence has at least two stages: identifying relevant information and verifying that information.[97] This section outlines the technologies and tactics that fact-finders are developing and deploying to integrate digital civilian witness information into their traditional human rights practices and to address the challenges this information poses. The security challenge crosscuts information evaluation as fact-finders endeavour to mitigate the new risks that digital reports pose to the information, its subjects, and its witnesses. The volume challenge is particularly a concern for the first stage of evaluation; the digital facilitation of collaboration and search functions supports expert sifting of the wheat from the chaff. The volume of this potentially relevant information, however, also poses a challenge for the verification stage. This is because verification is a time-intensive process centred on human expertise deployed against individual reports. ICTs can mitigate the verification challenge to a certain extent by supporting corroboration, including through the provision of 'verification subsidies' by third parties to the human rights

---

[94] Molly Land and others, *#ICT4HR: Information and Communication Technologies for Human Rights* (Rochester, NY: Social Science Research Network, 20 November 2012) <http://papers.ssrn.com/abstract=2178484>; Meier, 'From Crowdsourcing Crisis Information to Crowdseeding Conflict Zones (Updated)'.

[95] Land and others.

[96] Zittrain, Jonathan, 'The Internet Creates a New Kind of Sweatshop', *Newsweek*, 7 December 2009 <http://www.newsweek.com/internet-creates-new-kind-sweatshop-75751>.

[97] Jay D. Aronson, 'Crowd-Training Machine Learning Systems for Human Rights Abuse Documentation', in *Second AAAI Conference on Human Computation and Crowdsourcing: Workshop Citizen + X*, 2014 <www.aaai.org/ocs/index.php/HCOMP/HCOMP14/paper/viewFile/9267/9181>.

fact-finding process.[98]   This often depends, however, on sufficient digital verification literacy among human rights fact-finders and civilian witnesses, and consequently a number of projects address existing literacy lacunae.

Addressing the security challenge

Given the aforementioned risk of deletion for information circulating on social media, as well as the risk of corruption and obsolescence of digital data, various resources have been developed to assist human rights fact-finders with securely archiving their information. These include the extensive guide produced by Witness for activists on archiving video.[99]   Other examples are Martus, a system developed by Benetech for the digital organization, storage, backup and sharing of information, and OpenEvSys, a database application for recording, storing, searching, and analysing documented violations.[100]

The vulnerability of the subjects of digital civilian witness reports can be lessened through rendering identities as anonymous as possible. ObscuraCam is an Android app co-developed by The Guardian Project and Witness that allows users to pixelate faces in videos and photos.[101]   YouTube also has a face blurring feature.[102]   Though these initiatives may disguise subjects' identities and thus protect them from retribution, they still may not prevent re-victimization due to the circulation of the subject's suffering.[103]   The latter requires a broader consideration of the ethics of representation in human rights information and how they can be translated into civilian witness reporting applications.[104]

A number of ICT initiatives aim to reduce the risk of civilian witnesses arising from the moment of documentation, when they are in the same physical space as the perpetrator of the violation. These projects disguise the collection of information. Apps like Silent Lens, a concept arising from a Google 'Develop for Good' hackathon, allow users to secretly take photos while appearing to use the email or phone

[98] Ella McPherson, 'Source Credibility as "Information Subsidy": Strategies for Successful NGO Journalism at Mexican Human Rights NGOs' (working paper, 2015) <https://www.academia.edu/8157551/Credibility_as_Information_Subsidy_NGO_Journalism_at_Human_Rights_Organizations_in_Mexico>.

[99] Witness, 'Activists' Guide to Archiving Video', *Witness*, 2013 <http://archiveguide.witness.org>.

[100] Benetech, *Martus: Helping Human Rights Advocates Protect, Manage, and Effectively Utilize Information* (Benetech, n.d.) <www.martus.org/resources/Martus-Intro-Presentation-v50.pdf>; HURIDOCS, 'OpenEvsys – for Documenting Violations', *HURIDOCS*, 2015 <https://www.huridocs.org/openevsys/>.

[101] The Guardian Project, 'ObscuraCam: Secure Smart Camera', *The Guardian Project*, 2015 <https://guardianproject.info/apps/obscuracam/>.

[102] Sam Gregory, 'Visual Anonymity and YouTube's New Blurring Tool', *WITNESS Blog*, July 2012 <blog.witness.org/2012/07/visual-anonymity-and-youtubes-new-blurring-tool/>; Sameer Padania, 'Advocacy's Long and Winding Road', *Sameer Padania*, 2012 <http://blog.sameerpadania.com/2012/07/19/youtube-witness-face-blurring-advocacy/>; Youtube, 'Face Blurring: When Footage Requires Anonymity', *Official YouTube Blog*, 18 July 2012 <http://youtube-global.blogspot.com/2012/07/face-blurring-when-footage-requires.html>.

[103] Madeleine Bair, 'Abuse by Viral Video: Break the Cycle with Identity Protecting Tools', *WITNESS Blog*, August 2013 <https://blog.witness.org/2013/08/abuse-by-viral-video-break-the-cycle-with-identity-protecting-tools/>; Rutkin.

[104] Bair, 'Navigating the Ethics of Citizen Video: The Case of a Sexual Assault in Egypt'.

applications on their smartphones.[105] Videre Est Credere is an NGO that trains and equips activists in remote areas to use covert digital video cameras – hidden in items like pens, watches, and keyfobs – to document human rights violations.[106] Of course, like human rights defenders, civilian witnesses should ideally understand and be able to deploy the encryption and anonymity technologies outlined above to increase their security as they transmit their reports.

Addressing the volume challenge

The relevance of information to human rights fact-finding depends on a number of variables both particular to the case in question as well as universal – such as whether or not the information documents a violation and whether or not it contains the details necessary for verification. Addressing the volume challenge of digital information is about using human and machine power to intelligently winnow the relevant from the irrelevant. In other words, these initiatives tackle the 'signal-to-noise ratio' problem of social media and similar applications.[107]

Human power can be harnessed through the digital enablement of collaboration, as in the crowdsourcing done by the Standby Task Force. This is a network of trained volunteers – 'digital humanitarians' – who deploy digital skills in support of crisis-affected communities, including human rights crises.[108] These volunteers, a bounded crowd, support the collaborative evaluation of information through, for example, tagging government tanks in satellite images of Syria.[109] By splicing expert tasks into microtasks, relatively amateur crowds can analyse aspects of large quantities of information quickly. That said, the participants are necessarily limited to simpler tasks such as feature-spotting, and even then they pose risks of omissions due to inexperience; the Standby Task Force analysis therefore involved expert oversight from Amnesty International USA.[110] Another approach for sifting

> **Syria Right Now**
>
> *Eliot Higgins, expert on the analysis of social media information and founder of Brown Moses Blog and Bellingcat, is developing Syria Right Now. This application is a manually curated collection of social media accounts belonging to the Syrian opposition.*
>
> *Researchers wanting to know real-time information about an event in a particular place will be able visit Syria Right Now and instantly get a curated feed of original content from known sources related to that location. As Higgins describes it, 'Ultimately I want to change the discovery stage for examining social media from Syrian opposition areas from something that can take hours to something that's a few mouse clicks, and even have the content come and find you. Then more time can be spent on verification rather than finding something worth verifying' (Eliot Higgins, personal communication, 7 January 2015).*

---

[105] Silent Lens, 'Silent Lens', *Silent Lens*, n.d. <http://silentlens.com>.

[106] David James Smith, 'Videre: The Secretive Group on a Mission to Film Human-Rights Abuses', *Wired UK*, 29 August 2013 <http://www.wired.co.uk/magazine/archive/2013/09/features/videre>.

[107] Dan King, 'Using SwiftRiver to Find the Needle in the Social Media Haystack', *Ushahidi*, 2014 <www.ushahidi.com/2014/12/09/using-swiftriver-find-needle-social-media-haystack-2/>.

[108] Standby Task Force, 'What We Do', *Standby Task Force*, n.d. <http://blog.standbytaskforce.com/our-model/what-we-do/>.

[109] Patrick Meier, 'Combining Crowdsourced Satellite Imagery Analysis with Crisis Reporting: An Update on Syria', *iRevolutions*, 19 September 2011 <http://irevolution.net/2011/09/19/crowdsourcing-update-on-syria/>.

[110] Wang and others.

digital information is manual curation, as employed by the Syria Right Now project in its selection and geolocation of social media sources.

Machine power can be harnessed through enabling and automating data cleansing and search functions on large datasets of potentially relevant information. CrisisNET, a Ushahidi project funded by the Rockefeller Foundation is a 'firehose of global crisis data' based on its collection and standardization of real-time digital crisis data for individual researchers to search quickly and efficiently.[111] This platform, currently in beta, draws on thousands of sources producing information pertinent to crises, such as social media, Ushahidi crowdmaps, news outlets, and UNHCR refugee reports.[112]

Addressing the verification challenge

Once relevant information has been identified, it must be verified. Though the nature of the information being verified and the techniques and tools for verification are shifting rapidly as ICTs evolve, the fundamentals of verification remain constant: identifying and corroborating the content and the metadata of the information using a variety of methods and sources. Given the subjective nature of facticity, verification remains a human – indeed expert – practice.[113]

Nevertheless, digital tools are in development to speed and simplify this process. This section first outlines steps of the verification practice and the tactics of digital information forensics developed to address them. It goes on to examine the specific category of third parties 'verification subsidies,' developed to enhance the metadata of civilian witnesses' information or to take on some of the verification labour.[114] The section concluded by outlining some of the initiatives underway to boost digital literacy around verification – a challenge when many witnesses are spontaneous and many NGOs' resources are already strained.[115]

The fundamentals of verification and digital information forensics

The verification of digital information from civilian witnesses can be a long and complicated process.[116] Digital information forensics is an area of expertise that combines digital tools and databases with traditional gumshoe verification tactics.[117]

---

[111] CrisisNET, 'Frequently Asked Questions', *CrisisNET*, 2014 <blog.crisis.net/frequently-asked-questions/>.

[112] CrisisNET.

[113] Aronson; McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'; Craig Silverman and Rina Tsubaki, 'When Emergency News Breaks', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 5–12 <http://verificationhandbook.com/book/chapter1.php>.

[114] McPherson, 'Source Credibility as "Information Subsidy": Strategies for Successful NGO Journalism at Mexican Human Rights NGOs'.

[115] Hankey and Clunaigh; McPherson, II.

[116] Silverman and Tsubaki.

[117] Patrick Meier, 'How to Verify Social Media Content: Some Tips and Tricks on Information Forensics', *iRevolutions*, 21 June 2011 <http://irevolution.net/2011/06/21/information-forensics/>.

These tactics focus on cross-referencing the provenance, source, time and place of the information. These may be particularly difficult to establish for digital information, as it can be relatively disembodied from the source and context of its production.

Unearthing a piece of information's provenance is about establishing the chain-of-custody of the information and tracing it back to the original source. This step helps check that the content and its metadata have not been altered or manipulated – especially given the prevalent practice on YouTube of 'scraping' or recycling content without attribution.[122] Reverse image search applications like those provided by Google or TinEye can help; users can upload or link to an image, and these applications will return the locations of matching copies.[123]

> ***Documenting a Boko Haram attack in Nigeria using satellites***
>
> *Fact-finders at Amnesty International and at Human Rights Watch undertook change detection analysis of satellite images of two towns in north-eastern Nigeria on the 2nd and 7th of January, 2015.[118] These revealed extensive destruction from fire damage. Researchers cross-referenced this information with eyewitness testimonies to establish that the fires were part of attacks by Boko Haram militants on these towns in which hundreds were killed.[119] This cross-referencing of satellite images is important as, on their own, these remote images do little to establish culpability and causality.[120] This case was a 'text book example' of what satellite images can do for human rights fact-finding, both in terms of remote sensing hard-to-reach areas and in terms of producing powerful imagery for advocacy in the form of before-and-after pictures.[121]*

The fact-finder should ideally speak with the original source to assess her story of witnessing and documenting the event.[124] Verification experts recommend that fact-finders then examine the source's digital footprint for organizational affiliations, posting history, followers and friends, and location.[125] For example, the longevity of a social media account may

---

[118] Mausi Segun, 'Dispatches: What Really Happened in Baga, Nigeria?', *Human Rights Watch*, 14 January 2015 <http://www.hrw.org/news/2015/01/14/dispatches-what-really-happened-baga-nigeria>; Amnesty International, 'Nigeria: Satellite Images Show Horrific Scale of Boko Haram Attack on Baga', *Amnesty International*, 15 January 2015 <www.amnesty.org/en/news/nigeria-satellite-images-show-horrific-scale-boko-haram-attack-baga-2015-01-15>.

[119] Amnesty International, 'Nigeria: Satellite Images Show Horrific Scale of Boko Haram Attack on Baga'; Christoph Koettl, 'The Story behind the Boko Haram Satellite Images', *Amnesty International UK / Blogs: Into the Ether*, 2015 <www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satellite-images>.

[120] Wang and others.

[121] Koettl, 'The Story behind the Boko Haram Satellite Images'.

[122] Claire Wardle, 'Verifying User-Generated Content', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 24–33 <http://verificationhandbook.com/downloads/verification.handbook.pdf>.

[123] Trushar Barot, 'Verifying Images', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 33–44 <verificationhandbook.com/book/chapter4.php>.

[124] Barot.

[125] Malachy Browne, 'Verifying Video', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 45–67 <verificationhandbook.com/book/chapter5.php>; Della Kilroy, 'Citizen Video for Journalists: Verification', *WITNESS Blog*, 25 February 2013 <blog.witness.org/2013/02/citizen-video-for-journalists-verification/>; Meier, 'How to Verify Social Media Content'; Silverman and Tsubaki.

indicate credibility, because misinformation is often posted to new accounts.[126] Because it delves the 'deep web' of databases like public records and online profiles not currently indexed by mainstream search engines, pipl.com can facilitate this.[127] As Wardle warns, however, 'there is no quick way' of verifying the identity of a social media account; rather, this it requires 'painstaking checks,' akin to 'old-fashioned police investigation.'[128]

The next stage is verifying the time and place of production. Fact-finders may identify this metadata when they speak to the source, or it may be evident in the information. The source may have included it as part of production, such as by stating the location and date on camera, or as part of transmission, such as by providing commentary upon upload to YouTube. Clues about time and place may stem from landmarks, shadows, weather, signage, clothing, weapons, and dialect captured in the content.[129] It may also be automatically embedded in the file, such as in the timestamp; digital applications, like FotoForensics and the Citizen Evidence Lab's YouTube Data Viewer, can facilitate the extraction of this metadata.[130]

Fact-finders can corroborate time and place with digital databases, which can easily be searched for landmarks (Google Maps) and weather histories (Wolfram Alpha).[131] Another source of digital data for corroboration is satellite images. Of course, all of this digital information can also be corroborated offline through on-the-ground research and by tapping into trusted and expert networks.[132]

As is clear from the above, corroboration through consulting other sources and methods is key to the verification process; a single source is not enough.[133] De Rosa explains it well: 'The information you're seeing on social media should be the first step toward trying to verify what actually occurred, rather than the final word.'[134] As such, it is clear that turning this information into evidence can require a significant amount of time and expertise.

---

[126] Christoph Koettl, 'Human Rights Citizen Video Assessment Tool', *Citizen Evidence Lab*, 2014 <fluidsurveys.com/s/citizenvideo-stress-test/>.

[127] pipl, 'Welcome to the Deep Web', *Pipl*, 2015 <https://pipl.com/help/deep-web/>; 'Verification Tools', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 108–10 <http://verificationhandbook.com/book/chapter10.php>.

[128] Wardle, pp. 29–30.

[129] Kilroy; Koettl, 'Human Rights Citizen Video Assessment Tool'.

[130] Barot; Christoph Koettl, 'YouTube Data Viewer', *Citizen Evidence Lab*, 2014 <citizenevidence.org/2014/07/01/youtube-dataviewer/>.

[131] Silverman, 'Verification Tools'.

[132] McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'.

[133] McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'.

[134] Anthony De Rosa, 'Using Social Media as a Police Scanner', *Verification Handbook*, 2014 <verificationhandbook.com/book/chapter2.1.php>.

Third party verification subsidies

Several initiatives are underway that reduce the amount of time needed by fact-finders and the amount of expertise needed by both fact-finders and civilian witnesses. These are verification subsidies provided by third parties, which – after Gandy's concept of 'information subsidies' – are strategies designed to make information easier to use.[135] Two categories of verification subsidies are considered here, those that enhance the metadata of civilian witnesses' digital information, and those that supplant some of fact-finders' verification labour. Each category includes both human and machine-powered initiatives.

In the first category of verification subsidies, one approach is to encourage civilian witnesses to include metadata at the point of transmission. The Syria Tracker project, for example, which crowdsources information about the conflict in Syria using the Ushahidi platform, requires submitters to enter a title, description, category of incident, and the location and time of reporting. Submitters also have the option of including digital images, contact information, and links to news sources and external video.[139]
Prompts like these have a knock-on effect of boosting civilian witnesses' verification

> ***Metadata-enhancement initiatives***
>
> ***CameraV:*** *Witness and the Guardian Project are using funding from the Knight Foundation's Knight News Challenge to develop CameraV, the public Android app based on their InformaCam platform. CameraV allows users to take photos or videos and then annotate them, notarize them with a unique identifier, and share them. It encrypts the stored files and can automatically embed them with metadata from the phone's GPS, Wi-Fi, and Bluetooth sensors.[136]*
>
> ***eyeWitness to atrocities***: *Developed by the International Bar Association, this app automatically embeds metadata into civilian witness video and photographs, then encrypts and locally stores this information with additional metadata that allows analysts to check for manipulation of content. The witness can send their photo or video with accompanying metadata to eyeWitness for storage and expert analysis.[137]*
>
> ***FotoAhora:*** *As protests in Venezuela grew in 2014, so did misinformation circulating on social media. In quick reaction, publicity company Mood Agency released FotoAhora, a Spanish-language app for iOS and Android that allows a user to take a photo and enter text on where they are and what is happening. The app then posts the image on the user's Twitter account with the hashtag #Venezuela. The Tweet also includes metadata gathered through the phone and a code that can be traced to ensure that the photo was captured with FotoAhora at the stated time and place.[138]*

---

[135] Oscar H. Gandy, *Beyond Agenda Setting: Information Subsidies and Public Policy* (Norwood, NJ: Ablex Pub. Co., 1982); McPherson, II.

[136] The Guardian Project, 'CameraV App and the InformaCam System', *CameraV*, 2015 <https://guardianproject.github.io/informacam-guide/en/InformacamGuide.html>; InformaCam, 'InformaCam - Secure & Verified Mobile Media', *InformaCam*, n.d. <guardianproject.info/informa/>.

[137] eyeWitness to atrocities, 'About', *eyeWitness to Atrocities*, 2015 <http://www.eyewitnessproject.org/> [accessed 17 September 2015].

[138] Madeleine Bair and Vienna Maglio, 'Photo, Video Verification Has Growing Role in Venezuela Protests', *WITNESS Blog*, 11 April 2014 <http://blog.witness.org/2014/04/growing-role-of-image-verification-in-venezuelas-protests/>; Grupo Mood C.A, 'FotoAhora', *App Store*, 2014 <itunes.apple.com/us/app/fotoahora/id824442402?l=es>.

[139] Syria Tracker, 'Submit a Report', *Syria Tracker*, n.d. <https://syriatracker.crowdmap.com/reports/submit>.

literacy. Other projects, like CameraV, eyeWitness to atrocities, and FotoAhora, automate metadata inclusion at the point of capture.[140]

In terms of verification subsidies that take on some of fact-finders' labour, one strategy is to harness the power of the crowd. An example is Veri.ly, a web-based project in development via collaboration between the University of Southampton, Masdar Institute, and QCRI. Veri.ly crowdsources verification by asking members of the public to corroborate or contradict a piece of information with textual or visual evidence.[141] The Citizen Media Evidence Partnership, a project being developed by Amnesty International's Sensor Project and Will H. Moore of Florida State University, also draws on a bounded crowd. This project trains student groups to become 'verification corps' dedicated to triaging information for verification by experts.[142] Other applications, such as Checkdesk, developed by social technology nonprofit Meedan and tailored for individual newsrooms, support collaborative and transparent team verification.[143]

Another strategy is to support the process of cross-referencing information against other sources and types of data. UC Berkeley CITRIS Data and Democracy is designing the Rashomon Project, for example, to facilitate the time-syncing of a number of civilian witness videos of the same incident so as to provide a 'multi-perspective video timeline.'[144] The Whistle, a project in development at the University of Cambridge, aims to automatically compare information inputted by civilian witnesses against information from some of the digital information forensics tools and databases listed above.[145]

Other projects are exploring the machine provision of verification subsidies for fact-finders. TweetCred, for example, developed by a team of academics from the Indraprastha Institute of Information Technology and the Qatar Computing Research Institute, attempts this through a machine-learning algorithm. TweetCred rates the credibility of individual Tweets real-time by evaluating them against 45 criteria. These include aspects of the Tweet's content – such as emoticons, swearwords, and

---

[140] eyeWitness to atrocities, 'About', *eyeWitness to Atrocities*, 2015 <http://www.eyewitnessproject.org/>; The Guardian Project, 'CameraV: Secure Verifiable Photo & Video Camera', *The Guardian Project*, 2015 <https://guardianproject.info/apps/camerav/>; Grupo Mood C.A.

[141] Victor Naroditskiy, 'Veri.ly - Getting the Facts Straight During Humanitarian Disasters', *Software Sustainability Institute*, 2014 <http://www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitarian-disasters>; Veri.ly, 'Is This Highgate Cemetery?', *Veri.ly*, 2014 <https://veri.ly/crisis/3/question/81-is-this-highgate-cemetery>.

[142] Koettl, '"The YouTube War"'; Will Moore, 'About', *Citizen Media Evidence Partnership (C-MEP)*, 2014 <http://c-mep.org/home/about/>.

[143] Dima Saber, *Checkdesk: Sorting, Developing & Disseminating Citizen Reporting in the MENA Region* (Birmingham City University and The University of Manchester, 2013) <https://www.academia.edu/8269524/Checkdesk_Sorting_Developing_and_Disseminating_Citizen_Reporting_in _the_MENA_Region>.

[144] The Rashomon Project, 'About Rashomon', *The Rashomon Project*, n.d. <http://rieff.ieor.berkeley.edu/rashomon/about-rashomon/>.

[145] The Whistle, 'About', *The Whistle*, 2015 <http://www.thewhistle.org>.

hashtags – as well as the metadata of the Tweet and information about its author, such as number of followers.[146]

Digital verification literacy

While digital information forensics and third party verification subsidies potentially speed the verification process, knowing about them does require some degree of digital verification literacy. Human rights fact-finders, driven by their field's culture of concern with methodology, can tap into networks of knowledge-exchange, and various projects offer resources for human rights fact-finders to build their digital verification expertise. For example, the Verification Handbook, published in 2014 by the European Journalism Centre, gathers insight from leading verification experts and quickly became a reference point for human rights fact-finders, humanitarians, and journalists.[147] Amnesty's Citizen Evidence Lab is a knowledge exchange space for human rights fact-finders and defenders about using digital information.[148] Witness' Media Lab gathers together resources to inform the curation and verification of civilian witness videos.[149] New Tactics in Human Rights recently hosted an online conversation, publicly available and archived, on 'Using Video for Documentation and Evidence.'[150]

Resources designed for journalists can be equally relevant, given the core information value of veracity in both professions.[151] These include the BBC Academy website, targeted at professional journalists, and Eliot Higgins' Bellingcat website, targeted at citizen investigative journalists.[152] The blog by Storyful, a social media news agency now owned by News Corp, contain useful verification tactics and case studies.[153] Josh Stearns' Verification Junkie Tumblr blog collects digital verification tools.[154] First Draft News is an amalgamation of advice on using civilian witness information, and 2015 saw the publication of the Verification Handbook for Investigative Reporting.[155] The more knowledge about digital information forensics

---

[146] Aditi Gupta and others, 'TweetCred: A Real-Time Web-Based System for Assessing Credibility of Content on Twitter', in *Proceedings of Social Informatics (SocInfo 2014)*, 2014 <arxiv.org/abs/1405.5490>.

[147] *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014).

[148] Koettl, 'About & FAQ'.

[149] Witness, 'Witness Media Lab Resources', *Witness Media Lab*, 2015 <https://lab.witness.org/resources/>.

[150] New Tactics in Human Rights, 'Using Video for Documentation and Evidence', *New Tactics in Human Rights*, 2014 <https://www.newtactics.org/conversation/using-video-documentation-and-evidence>.

[151] McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'.

[152] BBC Academy, 'Social Media Verification: UGC Hub', *BBC Academy*, 2015 <http://www.bbc.co.uk/academy/journalism/skills/social-media/article/art20130702112133524>; Bellingcat, 'Home', *Bellingcat: By and for Citizen Investigative Journalists*, 2015 <https://www.bellingcat.com>.

[153] Storyful, 'Storyful Blog', *Storyful*, 2015 <http://blog.storyful.com/>.

[154] Josh Stearns, 'Verification Junkie', *Verification Junkie*, 2015 <http://verificationjunkie.com/?og=1>.

[155] First Draft News, 'About', *First Draft News*, 2015 <https://medium.com/1st-draft/about>; *Verification Handbook for Investigative Reporting: A Guide to Online Search and Research Techniques for Using UGC and Open Source Information in Investigations*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2015) <http://verificationhandbook.com/downloads/verification.handbook.2.pdf>.

that human rights fact-finders have, the more comfortably and quickly they will be able to use digital information from civilian witnesses.

Increasing verification knowledge among civilian witnesses is another way to facilitate the verification process. Witness, for example, provides a guide for individuals filming for human rights on what to include in their videos (and is also producing the related 'Visualize Justice: A Field Guide to Enhancing the Evidentiary Value of Video for Human Rights,' to be released soon).[156] The guide makes clear that investigators need to know the what, when, where, and – if safe – the who of the video. Accordingly, Witness provides sample scripts, slates, and other tactics that those filming can use to transmit these facts. As the guide explains, in the vein of verification subsidies:

> Adding this information to videos will make it much easier for reviewers that were not at the scene of the human rights incident to verify the content. Easier verification means there is a better chance that the video will be used to secure justice.[157]

Compared with knowledge-exchange among human rights fact-finders, it is less clear, however, how knowledge about producing and transmitting information effectively, safely, and ethically for evidence can diffuse among civilian witnesses, particularly those who are truly spontaneous.[158] As Gregory explains with reference to the spontaneous civilian witness who inspired the founding of Witness:

> …We know that today's version of George Holliday, the man who filmed the Rodney King incident, won't have a dedicated human rights app. And even if he does, if he's in a high-risk situation, it may help single him out as an activist.[159]

It is for this reason that Gregory advocates for the inclusion of an 'eyewitness' mode resembling InformaCam as standard in pre-installed photo and video tools on smartphones and in social media applications.[160] The mainstreaming of verification technologies means that civilian witnesses are more likely to know about them and thus to use them. That being said, volume and verification remain significant challenges for fact-finders' use of this information as evidence. Furthermore, one's ability to be a digital civilian witness, and to be relatively secure in doing so, is inflected by one's relative access to resources – an issue addressed in the conclusion of this report.

---

[156] Witness, 'Appendix: "VISUALIZE JUSTICE: A Field Guide to Enhancing the Evidentiary Value of Video for Human Rights"', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 109–12 <http://verificationhandbook.com/book/appendix.php>.

[157] Witness, "Video as Evidence."

[158] McPherson, ii.

[159] Sam Gregory, 'How An Eyewitness Mode Helps Activists (and Others) Be Trusted', *WITNESS Blog*, 3 March 2014 <blog.witness.org/2014/03/eyewitness-mode-helps-activists/>.

[160] Gregory, 'How An Eyewitness Mode Helps Activists (and Others) Be Trusted'.

ICTS AND THE HUMAN RIGHTS PRACTICE OF ADVOCACY

By communicating evidence, advocacy works hand-in-hand with fact-finding in the pursuit of human rights accountability. Advocacy is the systematic pursuit of particular causes, often via targeting individuals and institutions with information aiming to impel change.[161] This section looks in particular at two categories of advocacy targets: the wider public, whom advocacy aims to mobilize, and the individual target, whether a violator of human rights or someone in a position to put pressure on a violator. Human rights advocacy is more than just communicating evidence, however; it also includes the promotion of environments knowledgeable about and supportive of human rights – and thus receptive to advocacy.[162]

Human rights organizations are harnessing ICTs in their advocacy and promotion practices to benefit from particular affordances for communication and analysis. These comprise the abilities to communicate quickly, directly, publicly, and interactively with targets as well as to analyse the performance of messages and the nature and segmentation of audiences.[163] Such affordances are not exclusive to ICTs, as pre-existing communication channels allowed them as well, and human rights organizations tend to deploy digital and traditional communication tactics together.[164] ICTs such as social media, however, can make advocacy faster and cheaper.[165]

Of course, these affordances can also be hindrances for human rights advocacy with particular respect to broadening participation without deepening it and to creating new risks for the organizational reputations so important for its effectiveness. Meanwhile, ICTs may create new human rights educational opportunities, but these

---

[161] McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'; Aseem Prakash and Mary Kay Gugerty, 'Advocacy Organizations and Collective Action: An Introduction', in *Advocacy Organizations and Collective Action*, ed. by Aseem Prakash and Mary Kay Gugerty (Cambridge, UK: Cambridge University Press, 2010), pp. 1–28.

[162] Dustin N. Sharp, 'Human Rights Fact-Finding and the Reproduction of Hierarchies', in *Human Rights Fact-Finding in the 21st Century*, ed. by Philip Alston and Sarah Knuckey (Oxford, UK: Oxford University Press, Forthcoming) <http://papers.ssrn.com/abstract=2341186>.

[163] Chao Guo and Gregory D. Saxton, 'Tweeting Social Change How Social Media Are Changing Nonprofit Advocacy', *Nonprofit and Voluntary Sector Quarterly*, 43 (2014), 57–79 <http://dx.doi.org/10.1177/0899764012471585>; David Karpf, *The MoveOn Effect: The Unexpected Transformation of American Political Advocacy* (New York, NY: Oxford University Press, 2012); Kristen Lovejoy and Gregory D. Saxton, 'Information, Community, and Action: How Nonprofit Organizations Use Social Media', *Journal of Computer-Mediated Communication*, 17 (2012), 337–53 <http://dx.doi.org/10.1111/j.1083-6101.2012.01576.x>; Tim Norton, *Social Media Strategies for Advocacy and Targeted Communications* (Internews, 2013) <http://tim.anewleaf.com.au/files/2013/03/Social-Media-for-Advocacy-v1.pdf>; Jonathan A Obar, Paul Zube and Cliff Lampe, 'Advocacy 2.0: An Analysis of How Advocacy Groups in the United States Perceive and Use Social Media as Tools for Facilitating Civic Engagement and Collective Action', *Journal of Information Policy*, 2 (2012), 1–25.

[164] David Karpf, 'Online Political Mobilization from the Advocacy Group's Perspective: Looking Beyond Clicktivism', *Policy & Internet*, 2 (2010), 7–41; New Tactics in Human Rights, 'Incorporating Social Media into Your Human Rights Campaigning', *New Tactics in Human Rights*, 2013 <https://www.newtactics.org/conversation/incorporating-social-media-your-human-rights-campaigning>.

[165] Karpf, *The MoveOn Effect*.

are competing for attention in an ever-proliferating information context – and one that is only accessible to the digitally literate.[166]

Public mobilization

Optimism exists for digital human rights advocacy in part because ICTs allow human rights organizations to communicate direct-to-citizen, bypassing the traditional but often inscrutable public communication channels of the mainstream media. This largely untested optimism has fuelled innovation in a variety of advocacy practices harnessing social media and other applications for mobilizing the public.[168] ICTs are deployed for public mobilization in a variety of ways, including the two featured here: engaging the public in the visible amplification of advocacy messages and increasing the visibility of cases and issues, including those neglected by the mainstream media.

> ### #YaMeCansé and the enforced disappearance of 43 Mexican students
>
> *In September 2014, students from a rural teacher-training college in Ayotzinapa, Mexico, who were mobilizing to protest education conditions, got into a clash with police. Two were killed along with three bystanders, a third was found dead the next day, and the police abducted 43. At the time of publication, the charred remains of just a single student have been identified. Following an off-the-cuff remark by the Attorney General in a press conference about the case, 'Ya me cansé,' or 'I'm tired,' the hashtag #YaMeCansé surfaced on Twitter. Users stated that they too were tired of the state of affairs, including the 23,000 missing and 100,000 killed since the war on drugs started in 2006. This hashtag and its derivatives trended in Mexico for weeks and coincided with protests and other mobilization tactics. Still, the Mexican government declared the case closed in January 2015, despite protestations that there is not enough evidence yet to do so.[167]*

Human rights organizations have developed expertise in using social media to quickly and directly engage members of the public in their causes. The extent of the public's engagement in the advocacy message is rendered visible through their participation in likes, shares, re-tweets, and other numerical metrics on social media. The volume of participation, part of the advocacy strategy itself, is also evident in the automated aggregation of messages on social media applications through the use of hashtags. Among the most shared human rights tweets of 2014, for example, were those containing the hashtags #Ferguson, referencing the police shooting of Michael Brown and subsequent unrest there; #BringBackOurGirls, protesting the abduction of 200 schoolgirls by Boko Haram in Chibok, Nigeria; and

---

[166] A. Trevor Thrall, Dominik Stecula and Diana Sweet, 'May We Have Your Attention Please? Human-Rights NGOs and the Problem of Global Communication', *The International Journal of Press/Politics*, 19 (2014), 135–59 <http://dx.doi.org/10.1177/1940161213519132>.

[167] Amnesty International, 'Mexico: Investigation into the Enforced Disappearance of 43 Students Is far from Conclusive', *Amnesty International News*, 22 January 2015 <www.amnesty.org/en/news/mexico-investigation-enforced-disappearance-43-students-far-conclusive-2015-01-22>; BBC Trending, '"I Am Tired": The Politics of Mexico's #Yamecanse Hashtag', *BBC Trending*, 9 December 2014 <www.bbc.co.uk/news/blogs-trending-30294010>; Ella McPherson and Mónica Moreno Figueroa, 'Smoke, Mirrors and Murder: The Disappearance and Killing of Student Protesters in Mexico', *Red Pepper*, March 2015, pp. 36–37; Washington Office on Latin America, 'Too Early to Close the Ayotzinapa Case: Mexican Government's Actions Undermine Rule of Law', *Washington Office on Latin America*, 2015 <http://www.wola.org/news/too_early_to_close_the_ayotzinapa_case>.

[168] Thrall, Stecula and Sweet.

#CARCrisis, about the ongoing violence in Central African Republic.[169]   As social media metrics can convey the level of public interest in a campaign, they allow NGOs to have some measure of the effects of advocacy, which traditionally have been very difficult to isolate and expensive to test.[170]

Getting hashtags to trend is not just an organic process; rather, it often involves coordinated strategies. For example, Amnesty International USA used a number of social media tactics in its #MDRepeal campaign against the death penalty in Maryland. These included 'twitterbombing,' namely synchronising a number of Twitter users to tweet the same hashtag at the same time at the same target – in their case, the Twitter account of Maryland's governor. They also used 'Twitter chats,' coordinated Q&As about the topic, and 'livetweeting' events related to the repeal of the death penalty, which allowed the team to 'frame the story.'[171]

Various ICT applications exist to support public mobilization advocacy on social media.   Thunderclap, for example, a self-designated 'crowdspeaking platform,' allows users to donate their 'social reach' to share a single message in unison. Users give Thunderclap permission to post this message from their accounts. This happens simultaneously across all participating accounts only after the goal number of supporters has been reached.[172] For example, in 2014, the International Federation for Human Rights organized a thunderclap for the 17th of April, Syria's official Independence Day, stating: '#Syria: Free activists, media & humanitarian workers arbitrarily detained or abducted for their work #freeSYvoices http://thndr.it/1iGdclw.' Through the social media networks of 256 supporters, the thunderclap reached over two million people.[173]

Through such social media tools and strategies, the human rights community and interested members of the public aim to get or keep a case or issue on the public agenda. ICTs thus facilitate the visibility of human rights on a mass level – or at least those of the masses who are connected to social media. ICTs also facilitate the visibility of human rights on an individual level through the smartphones that are by many people's sides day and night. Apps, such as Amnesty's AiCandle, are, as Amnesty describes it, 'The fastest way to take action for human rights – at your fingertips.' This app allows users to take actions such as signing petitions and writing emails through their smartphones. These initiatives for 'Pocket Protest' – as another Amnesty project to quickly mobilize members by SMS message is called – can be

---

[169] Jim Murphy, 'Top 30 Human Rights Tweets of 2014', *Huffington Post*, 22 December 2014 <http://www.huffingtonpost.com/jim-murphy/top-30-human-rights-tweet_b_6366690.html>.

[170] Karpf, *The MoveOn Effect*; Gregory D. Saxton and others, '#AdvocatingForChange: The Strategic Use of Hashtags in Social Media Advocacy', *Advances in Social Work*, 16 (2015), 154–69.

[171] Jiva Manske, 'Case Studies: Concrete Examples of Compelling and Strategic Use of Social Media', *New Tactics in Human Rights*, 2013 <https://www.newtactics.org/comment/6124>.

[172] Thunderclap, 'Bringing the Thunder', *Thunderclap*, 2012 <https://www.thunderclap.it/casestudies>.

[173] International Federation for Human Rights, 'Thunderclap: Free Syria's Silenced Voices', *Thunderclap*, 2014 <www.thunderclap.it/projects/9773-free-syria-s-silenced-voices?locale=en>.

particularly useful for urgent mobilization, as members can be notified and can act instantly.[174]

Another visibility affordance of social media for human rights advocacy is its potential for highlighting cases and issues under-reported in the mainstream media. The ongoing conflict in the Central African Republic, for example, had received relatively little coverage in the English-speaking media. Peter Bouckaert, the head of the emergency team at Human Rights Watch, is credited with attracting some attention to the crisis by tweeting about events and atrocities that he witnessed on field visits, using the #CARcrisis hashtag.[175]

Direct targeting

Using social media can help the human rights community visibly engage publics, but they can also help channel these publics' outrage towards a particular target. Direct public targeting, whether the message is sent by a member of the public or a human rights organization, is relatively straightforward on social media. Users can, for example, mention the target in their tweets or post a comment on a target's Facebook page – provided the target has not elected to review visitor posts prior to publication.

> **#eyesonSyria**
>
> *Amnesty's multi-pronged 'Eyes on Syria' campaign used Twitter for direct targeting. Its aim was to persuade Russia to support efforts by the UN Security Council to put pressure on the Syrian Government. Amnesty requested that supporters tweet at Russian Prime Minister Dmitry Medvedev using the hashtag #eyesonsyria. Supporters were asked to do this in a specific two-hour window, and the hashtag briefly trended globally on Twitter.[176]*

These tactics may have particular windows of opportunity related to what some call the 'dictator's dilemma.'[177] This is understood as authoritarian regimes' choice of restricting online access and thus harming their economies versus broadly allowing online access and thus facilitating resistance.[178] The window of opportunity is when political targets are new to social media and thus new to the interactive and public nature of it that can facilitate public criticism. Regimes' sensitivity to public criticism may impel them to mitigate situations of human rights violations. Cuba, for example – where Internet use is very restricted – has released detained activists following campaigns on Twitter asking them to do so.[179] These windows of opportunity may

---

[174] Amnesty International, 'AiCandle on the App Store on iTunes', *iTunes*, 2011 <https://itunes.apple.com/gb/app/aicandle/id334420214?mt=8>; Amnesty International UK, 'What Is Pocket Protest?', *Amnesty International UK*, 2014 <www.amnesty.org.uk/what-pocket-protest>.

[175] Jared Malsin, 'Western Media: Stop Ignoring the Central African Republic Crisis', *Columbia Journalism Review*, 13 October 2014 <http://www.cjr.org/behind_the_news/western_media_stop_ignoring_th.php>.

[176] Manske.

[177] Clay Shirky, 'The Political Power of Social Media', *Foreign Affairs*, February 2011 <http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media>; Robertson and Olson, p. 39.

[178] Nivien Saleh, 'Egypt's Digital Activism and the Dictator's Dilemma: An Evaluation', *Telecommunications Policy*, 36 (2012), 476–83 <http://dx.doi.org/10.1016/j.telpol.2012.04.001>.

[179] Romero, p. 11.

close once governments become accustomed to digital flak and have strategies in place to deflect it.

Despite the affordances of ICTs for advocacy, the jury is still out as to whether they are markedly changing advocacy dynamics for the better – or changing them at all. First, this kind of public mobilization has been criticised as 'clicktivism,' a 21st century version of armchair activism. Gladwell, for example, describes social media activism as composed of weak ties good for the spread of information, whereas 'high-risk activism' – which actually impels change – needs strong ties. 'Social networks are effective at increasing *participation*,' he writes, 'by lessening the level of motivation that participation requires.'[180]   Furthermore, the demands arising from such participation may be misguided because the brevity of social media formats stymies a full understanding of the scenario.[181]   Another problem, not limited to but rather reproduced in digital advocacy, is the imbalance between who advocates versus whom is advocated about. Both the #StopKony campaign, a 2012 social media project by NGO Invisible Children advocating for the capture of Ugandan warlord Joseph Kony, and 2014's #Bringbackourgirls, a viral hashtag protesting extremist group Boko Haram's kidnapping of Nigerian schoolgirls, have been critiqued for their neo-imperialistic overtones.[182]   Others are quick, however, to defend digitally-enabled pluralism in human rights advocacy. For example, Vie applauds the Human Rights Campaign's marriage equality meme, a red box containing a pink equals sign, which Facebook users adopted en masse as their profile pictures in 2013. Vie argues that such 'seemingly insignificant moves' are significant in their accumulation through demonstrating a 'supportive environment' and through 'drawing awareness.'[183]

Second, of concern here as well is the mediatisation of human rights advocacy, in which advocacy practices are altered – not necessarily for the better – in response to the rising prominence of social media in advocacy. For example, the affordance of user analytics is, on the one hand, useful for demonstrating the extent of the public's engagement with an issue. On the other hand, the more campaigns are focused around participation numbers, the greater the risk of focusing on 'popular' human rights issues to the detriment of more complicated and less compelling issues – at least with respect to the brief and visual language of social media communications.[184]

---

[180] Malcolm Gladwell, 'Small Change: Why the Revolution Will Not Be Tweeted', *The New Yorker*, 4 October 2010 <www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell>.

[181] Johanna Herman, 'Hashtags and Human Rights: Activism in the Age of Twitter', *Carnegie Council for Ethics in International Affairs*, 2014 <www.carnegiecouncil.org/publications/ethics_online/0099>.

[182] Caitlin Dewey, '#Bringbackourgirls, #Kony2012, and the Complete, Divisive History of "Hashtag Activism"', *The Washington Post*, 8 May 2014 <www.washingtonpost.com/news/the-intersect/wp/2014/05/08/bringbackourgirls-kony2012-and-the-complete-divisive-history-of-hashtag-activism/>; Meredith Loken, '#BringBackOurGirls and the Invisibility of Imperialism', *Feminist Media Studies*, 14 (2014), 1100–1101 <http://dx.doi.org/10.1080/14680777.2014.975442>.

[183] Stephanie Vie, 'In Defense of "slacktivism": The Human Rights Campaign Facebook Logo as Digital Activism', *First Monday*, 19 (2014) <http://firstmonday.org/ojs/index.php/fm/article/view/4961>.

[184] Sharp.

Third, social media's affordance of virality, allowing for the rapid spread of information, can sit uneasily with human rights evidence and traditional human rights advocacy. This is because virality tends to be correlated to messages of hope, humour, and shock. Still, human rights advocacy can go viral, as exemplified by aid organization Plan's controversial 2014 campaign highlighting the plight of child brides. This campaign successfully harnessed the mechanism of shock; its fake blog purportedly written by 'Thea,' a 12-year-old Norwegian girl, about her impending marriage to 37-year-old Geir, has attracted more visits than any other blog in Norway.[185]

Fourth, social media's affordance of speed, which underpins virality, creates the risk of errors. Errors are detrimental to human rights organizations' reputations for credibility and thus imperil the effectiveness of their advocacy. Interactivity, which facilitates relationship-building with members and publics, also opens the door for public critique. This can particularly problematic in the early stages of adoption, before organizations have built up online user communities that naturally tend to monitor NGOs' profiles, responding to criticisms.[186] Here, as with all the uses of ICTs for human rights, digital literacy is clearly needed.

Human rights promotion

Supporting individuals' knowledge about human rights is part of promoting a culture that values and safeguards rights and responds to their violation. ICTs create new channels and applications – including web resources, mobile apps, and games – for raising awareness of rights and the mechanisms for protecting and defending them. The web interface Human Rights Atlas, for example, developed by the University of Essex and partners, allows users to easily search for demographic indicators, human rights legal commitments, and human rights performance at the country level.[189]

> **The Universal Adventure of Human Rights: Interplanetary Mission**
>
> *This online game (La Aventura Universal de los Derechos Humanos: Misión Interplanetaria) was developed by Caja Madrid Obra Social, the foundation arm of the Caja Madrid savings bank. It is targeted at 6 to 12 years olds and is designed to introduce them to the articles of the Universal Declaration of Human Rights.[187] For example, to learn about Article 3's 'right to life, liberty and security of person,' the player travels to Planet Life to rescue extraterrestrials from their pursuers.[188]*

Complementary to this provision of data is the focus among other web resources on the provision of human rights education. 'International Human Rights' is a free

---

[185] Rachel Nuwer, 'The Fake Story of a Blond Child Bride Made This the Most Visited Blog in Norway', *Smithsonian*, 8 October 2014 <http://www.smithsonianmag.com/smart-news/fake-story-blond-child-bride-made-most-visited-blog-norway-180952977/>.

[186] Norton.

[187] Caja Madrid Obra Social, 'Padres Y Tutores', *La Aventura Universal de Los Derechos Humanos: Misión Interplanetaria*, n.d. <www.aventurauniversal.com/tutores.asp>.

[188] Caja Madrid Obra Social, 'Capítulo 1', *La Aventura Universal de Los Derechos Humanos: Misión Interplanetaria*, n.d. <www.aventurauniversal.com/juego1.asp>.

[189] Todd Landman, 'Resources', *Human Rights Atlas*, 2015 <www.humanrightsatlas.org/resources/>.

online course available as a massive open online course (MOOC) hosted on platform edX.[190] Nonprofit Youth for Human Rights has developed an educational iPad and iPhone app for school-age students that will soon be provided in more than a dozen languages.[191] Games targeting children aim to teach human rights through play. These initiatives promoting human rights draw on the affordances of ICTs for analytics, interactivity, and even portability. They go some way towards fostering the ubiquity of human rights ideas among users around the world. That said, this exposure to human rights knowledge, and the benefits it brings to individuals seeking to protect themselves, is available largely to citizens on one side of digital divides.

---

[190] Olivier De Schutter, 'International Human Rights', *edX*, 2015 <www.edx.org/course/international-human-rights-louvainx-louv2x>.

[191] Youth for Human Rights International, 'Youth for Human Rights Online Education App', *Youth for Human Rights Online Education*, 2015 <http://education.youthforhumanrights.org/edu-translated.html>.

CONCLUSION: A RESEARCH FRAMEWORK FOR APPROACHING ICTS AND HUMAN RIGHTS PRACTICE

This report has provided a snapshot of the use of ICTs in human rights practice, a fast-paced area in which understanding and literacy lag developments on the ground. This report aims to shorten this lag and to provide a foundation for academics and practitioners interested in this space. In terms of prevention, ICTs can be harnessed to protect human rights defenders, to prevent violations in police-civilian interactions, and in data-driven early warning systems and communication-based conflict prevention. That being said, the use of ICTs also creates new security risks for HRDs and can violate the right to privacy. In terms of fact-finding, ICTs afford the spontaneous and solicited participation of civilian witnesses in the production of human rights evidence. Of course, a greater volume and variety of information from unknown and untrained sources creates problems of misinformation and verification, which technology only goes so far to mitigate. In terms of advocacy, ICTs provide new channels for quickly and visibly mobilizing publics, for directly engaging with advocacy targets, and for spreading awareness of human rights. The effects of these new advocacy channels are unclear, however, and they may imperil categories of human rights and the reputations of human rights organizations.

The opportunities outlined here are a cause for optimism, but the risks show that the use of ICTs should be approached with an abundance of caution and an understanding of context – and that the best decision on the ground may be to not use them at all. In any case, their adoption should be evaluated for opportunities and risks not only against existing practices, but also in terms of how and why these opportunities and risks are distributed. Given this report's mandate to map the terrain, it has focused on identifying the opportunities and risks of categories of ICT initiatives and trends. A full understanding of the topic should not, however, stop at this first stage of research. A fruitful second stage of research involves considering how digital divides differentially distribute the benefits of the opportunities and the burdens of the risks among populations. A beneficial third stage requires examining how the political economy of initiatives and their contexts can inflect the extent and the distribution of both digital divides and ICTs' risks and opportunities in human rights practice. It is worth taking a moment here to outline both of these research stages in more detail.

ICTs and digital divides

The concept of the digital divide refers to the distinction between those who do and those who do not have access to new ICTs; more recently, it also refers to those who do and those who do not have the digital literacy necessary to take advantage of new ICTs.[192] So far in this report, we have outlined many of the opportunities and

---

[192] David J. Gunkel, 'Second Thoughts: Toward a Critique of the Digital Divide', *New Media & Society*, 5 (2003), 499–522 <http://dx.doi.org/10.1177/146144480354003>.

risks related to the use of ICTs in the core human rights practices of prevention, fact-finding, and advocacy. Digital divides impact who benefits from these opportunities and who suffers from these risks. On the one hand, ICTs can facilitate the pluralism of human rights practice, namely the volume and variety of voices involved, particularly in terms of amateurs and closed contexts. This is a shift that is in line with the inclusive ethos of human rights.[193] On the other hand, new digital initiatives create new lines of inclusion and exclusion inflected by access to and knowledge of technologies. These lines often correspond with other registers of access to resources and power.

This is evident in identifying who can and cannot benefit from the digitally-enabled prevention initiatives outlined earlier. To gain from these, human rights practitioners need to know about the risks of ICTs and how to protect themselves. In the context of optimism among human right practitioners about the benefits of ICTs, risks may not get the attention they deserve. As a practitioner at an organization that trains other defenders on digital security told me: 'A lot of them don't know that Facebook is where a lot of people who would target human rights defenders go shopping.' Police body-worn cameras may be effective for reducing the violence in police-civilian interactions, but the livestream documentation that is part of their effectiveness may not work exactly where it is most needed. Low-income areas in Brazil, for example, tend to be where issues of patchy mobile coverage are concentrated.[194]

In terms of fact-finding, social media has created a wealth of opportunities for civilians to speak on situations of human rights violations they have witnessed. Pluralism is not just about speaking, however, but also about being heard.[195] Being heard by a human rights fact-finder often depends on one's ability to produce verifiable information, which is facilitated by having a well-networked digital footprint and strong digital verification literacy. Verification thus may be a barrier for less-resourced civilian witnesses to accessing human rights accountability.[196] The standardization of the 'eyewitness mode' referenced above holds promise in part because it requires so little expertise from civilian witnesses. That said, even this option for reporting violations excludes those who are not online. Digital divides exist not only among civilian witnesses, but also among human rights fact-finders; the increasing necessity of technological expertise for information forensics is consolidating that expertise among the well-funded Western NGOs.[197]

---

[193] Scott Edwards and Christoph Koettl, 'The Amnesty Crowd: Mapping Saudi Arabia', *Ushahidi*, 20 June 2011 <www.ushahidi.com/2011/06/20/amnesty-crowd/>; Molly Land, 'Participatory Fact-Finding: Developing New Directions for Human Rights Investigations Through New Technologies', in *The Future of Human Rights Fact-Finding*, ed. by Philip Alston and Sarah Knuckey (Oxford, UK: Oxford University Press, Forthcoming).

[194] Liza Booth, 'Can Technology Catch Criminals in Brazil?', *SmartPlanet*, 2014 <www.smartplanet.com/blog/global-observer/can-technology-catch-criminals-in-brazil/>.

[195] Matthew Hindman, *The Myth of Digital Democracy* (Princeton, NJ: Princeton University Press, 2010).

[196] McPherson, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models'; McPherson, II.

[197] Satterthwaite and Simeone; Sharp.

ICTs can enable a greater variety and volume of voices in human rights advocacy, in part because of the ease with which digitally-endowed and digitally-literate publics can show their support for particular causes. The promotion of human rights using ICTs may indeed contribute to a culture of awareness, but if promotion resources for these initiatives are diverted away from more traditional channels, this is to the detriment of vulnerable groups who are not online. Furthermore, as with fact-finding, not all voices in online advocacy are heard equally – not just because of digital divides, but also more generally because of access to resources and power. For example, optimism about ICTs levelling the public sphere playing field would indicate that smaller human rights NGOs would gain voice vis-à-vis larger ones, and that human rights NGOs as a category would gain vis-à-vis more powerful sectors. A recent study, however, found that, of 257 sampled human rights NGOs, 10 percent had 92 percent of the group's total Twitter followers, 90 percent of the group's views on YouTube, and 81 percent of their likes on Facebook. Clearly, the rise of ICTs has not re-distributed attention between NGOs. Nor, the study found, has it helped NGOs set the agenda in the mainstream media.[198]

Digital divides cut through populations all over the map based on all kinds of characteristics. Language is one of them. Apps are often written and coded in English, and the emphasis on the written word in the design of ICTs disadvantages oral cultures.[199] Furthermore, access to technology may be embedded in power relations at the local level, such as according to gender and position within the social hierarchy.[200] It may also play into power relations on a larger scale, at the levels of urban versus rural, educated versus uneducated, and wealthy versus poor.[201] These digital divides shape the distribution of opportunities and risks in the use of ICTs in human rights practice. Digital divides, in turn, are delineated by power relations related to the production and use of technology.

The political economy of ICTs

Understanding the political economy of a practice or resource means understanding the power relations that shape that practice or resource.[202] In the case of ICTs relevant to human rights, we can examine, among other aspects, the ownership and control of these ICTs. Those who own and control ICTs set the parameters for the opportunities these ICTs afford for human rights practices and the risks they present; they also contribute to the contours of digital divides. Because of the oft-significant costs of developing and building ICTs, they tend to be owned and therefore

---

[198] Thrall, Stecula and Sweet, p. 143.

[199] Gwyneth Sutherlin, 'Letters: The Problem with Mapping Hate Speech', *Foreign Policy*, 11 April 2013 <http://foreignpolicy.com/2013/04/11/letters-the-problem-with-mapping-hate-speech/>.

[200] Land and others.

[201] United Nations Office for the Coordination of Humanitarian Affairs, *Humanitarianism in the Network Age*, OCHA Policy and Studies Series (New York, NY: United Nations Office for the Coordination of Humanitarian Affairs, 2013) <https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf>.

[202] Vincent Mosco, *The Political Economy of Communication*, 2nd edn (London, UK: SAGE Publications Ltd, 2009).

controlled by commercial players or states. These entities' incentives are not necessarily aligned with those of the human rights community. HRDs have thus also struck out on their own to create ICTs with support from funders and developers.

This does not mean that collaborations and conversations between technology companies and the human rights community have not been fruitful; YouTube installed its face blurring tool, for example, following advocacy by Witness.[203] Companies have their own prerogatives, however, not least of which are their commercial goals. These prerogatives may cause companies to regulate or change the platforms and applications on which the human rights community depends.[204] As mentioned, social media companies may remove posts documenting violations in response to political pressure or because they contravene community standards about graphic content.[205] In another example, core to the business model of a number of technology companies that trade in information are the algorithms that sift that data. In part because of their commercial value, the workings of these algorithms are often opaque – yet they can have tremendous impact on what is seen, heard, and read in the public sphere.[206] This has implications for human rights advocacy, as these algorithms influence its visibility. Algorithms may also affect the nature of human rights advocacy if HRDs alter advocacy's content and style based on what they anticipate that algorithms reward.[207] It is no wonder that a push for algorithmic accountability is gathering steam amongst the academic and journalistic communities.[208]

State control of ICTs may be a function of ownership, but it also may be a function of regulation or repression. Sometimes this is outright, as in the recent allegations of government shutdowns of the internet in Libya, Egypt and Syria.[209] Alternatively, states can use their ability to block websites to pressure social media companies to censor particular content.[210] China's extensive and complex system of censorship, known colloquially as the Great Firewall of China, does indeed block externally-owned commercial social media, such as Twitter, Facebook, and YouTube. Sina Weibo, a Chinese social media company that requires users to register with their real

---

[203] Gregory, 'Visual Anonymity and YouTube's New Blurring Tool'.

[204] William Lafi Youmans and Jillian C. York, 'Social Media and the Activist Toolkit: User Agreements, Corporate Interests, and the Information Infrastructure of Modern Social Movements', *Journal of Communication*, 62 (2012), 315–29 <http://dx.doi.org/10.1111/j.1460-2466.2012.01636.x>.

[205] Bair, 'Navigating the Ethics of Citizen Video: The Case of a Sexual Assault in Egypt'; Padania and others; Michael Pizzi, 'The Syrian Opposition Is Disappearing from Facebook', *The Atlantic*, 4 February 2014 <http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/>.

[206] Zeynep Tufekci, 'What Happens to #Ferguson Affects Ferguson', *Medium*, 14 August 2014 <https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0>.

[207] Victor Luckerson, 'Here's How Your Facebook News Feed Actually Works', *Time*, 9 July 2015 <http://time.com/3950525/facebook-news-feed-algorithm/>.

[208] Nicholas Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes* (New York, NY: Columbia Journalism School Tow Center for Digital Journalism, 2013) <http://www.nickdiakopoulos.com/wp-content/uploads/2011/07/Algorithmic-Accountability-Reporting_final.pdf>.

[209] Nicholas Thompson, 'Why Did Syria Shut Down the Internet?', *The New Yorker*, 2013 <http://www.newyorker.com/news/daily-comment/why-did-syria-shut-down-the-internet>.

[210] Youmans and York.

names, is a popular alternative, but is heavily monitored, censored, and flush with state propaganda.[211]   Furthermore, states such as the U.S. and the U.K. have a history of pushing technology companies to build backdoor access into encryption technologies for them.[212]

The third sector also exerts a measure of control on ICTs used in human rights work, whether through design, funding, or donations in kind. On the one hand, this can allow the human rights community more autonomy to develop and deploy – and possibly even to commercialize – ICTs, as evidenced by existing collaborations with ICT specialists such as those undertaken by HURIDOCS.[213]   On the other hand, this can tie HRDs' hands, as when donors are more interested in funding the technology than the training, creating risks for untrained users.[214]   As with ICT4D (ICTs for development) projects, which have been criticised for imposing Northern ideas on Southern peoples, ICT4HR projects are much improved through a critical-reflexive examination of the power relations they themselves may draw upon and generate.[215] This examination should form part of the research that developers and users of ICTs in the human rights space should undertake as part of their due diligence in the name of human rights.

ICTs create opportunities for human rights work beyond those outlined in this report, including coordinating work, crowdsourcing solutions to human rights issues, gathering opinions on the priorities of human rights practice, and facilitating extra-institutional civilian fact-finding.[216]   The future no doubt imminently heralds new applications, and this report is therefore accompanied by a student run blog, ictandhr.tumblr.com, that welcomes submissions.   The sum of these digitally-enabled opportunities for pluralism increases 'social accountability,' or the mechanisms that a citizen has to hold her government to account – that is, a citizen with the literacy, time, and money to engage with ICTs.[217]

Going forward, research should build on this report's development of the first stage of the research framework for approaching ICTs and human rights practice to delve further into stages two and three. For example, a fuller understanding of the political economy of an ICT and its use would involve understanding not only economic and political ownership and control, but also power relations within the

---

[211] Freedom House, *Freedom of the Net: China* (Freedom House, 2014) <freedomhouse.org/report/freedom-net/2014/china>; Gary King, Jennifer Pan and Margaret Roberts, 'Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation', *Science*, 345 (2014), 1–10.

[212] Danielle Kehl, Andi Wilson and Kevin Bankston, *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s* (Open Technology Institute, CyberSecurity Initiative, 2015) <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/OTI_Crypto_Wars_History.abe6caa19cbc40de842e01c28a028418.pdf>.

[213] Himelfarb and Varghese; HURIDOCS, 'Research & Development', *HURIDOCS*, 2015 <https://www.huridocs.org/research-development/>.

[214] Romero.

[215] Don Slater, *New Media, Development and Globalization: Making Connections in the Global South* (Cambridge, UK: Polity, 2014).

[216] Land, 'Participatory Fact-Finding: Developing New Directions for Human Rights Investigations Through New Technologies'.

[217] Land and others.

culture and the social organization of relevant practices and institutions.[218] Beyond presenting a fuller picture, approaching ICTs through this framework sets researchers and practitioners on a pathway to action. Exposing digital divides can lower barriers to pluralism, which researching the political economy leading to these digital divides can shed light on abuses of power; both of these actions are core goals of the human rights community. Critical and reflexive ICT design, policy-making, and awareness-raising thus have the potential to further ICTs' contributions to human rights on the ground as well as in spirit.

---

[218] Michael Schudson, 'The Sociology of News Production Revisited (Again)', in *Mass Media and Society*, ed. by James Curran and Michael Gurevitch, 3rd edn (London, UK: Arnold, 2000), pp. 175–200.

BIBLIOGRAPHY

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze, Whitfield Diffie, and others, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, Computer Science and Artificial Intelligence Laboratory Technical Report, 6 July 2015 <http://www.cl.cam.ac.uk/~rja14/Papers/doormats.pdf>

Access, 'Access Tech', *Access* <https://www.accessnow.org/pages/tech#Digital%20Security%20Helpline>

Alston, Philip, 'Introduction: Third Generation Human Rights Fact-Finding', in *Proceedings of the Annual Meeting (American Society of International Law)*, 2013, CVII, 61–62

Amnesty International, 'AiCandle on the App Store on iTunes', *iTunes*, 2011 <https://itunes.apple.com/gb/app/aicandle/id334420214?mt=8>

———, 'Legal and Research Tools', *Amnesty International*, 2015 <www.amnesty.org/en/human-rights-defenders/resources/legal-and-research-tools>

———, 'Mexico: Investigation into the Enforced Disappearance of 43 Students Is far from Conclusive', *Amnesty International News*, 22 January 2015 <www.amnesty.org/en/news/mexico-investigation-enforced-disappearance-43-students-far-conclusive-2015-01-22>

———, 'Nigeria: Satellite Images Show Horrific Scale of Boko Haram Attack on Baga', *Amnesty International*, 15 January 2015 <www.amnesty.org/en/news/nigeria-satellite-images-show-horrific-scale-boko-haram-attack-baga-2015-01-15>

Amnesty International UK, 'What Is Pocket Protest?', *Amnesty International UK*, 2014 <www.amnesty.org.uk/what-pocket-protest>

Aronson, Jay D., 'Crowd-Training Machine Learning Systems for Human Rights Abuse Documentation', in *Second AAAI Conference on Human Computation and Crowdsourcing: Workshop Citizen + X*, 2014 <www.aaai.org/ocs/index.php/HCOMP/HCOMP14/paper/viewFile/9267/9181>

Ashenfelder, Mike, 'Social Media Networks Stripping Data from Your Digital Photos', *The Signal: Digital Preservation, Library of Congress Blog*, 2013 <blogs.loc.gov/digitalpreservation/2013/04/social-media-networks-stripping-data-from-your-digital-photos/>

Bair, Madeleine, 'Abuse by Viral Video: Break the Cycle with Identity Protecting Tools', *WITNESS Blog*, August 2013 <https://blog.witness.org/2013/08/abuse-by-viral-video-break-the-cycle-with-identity-protecting-tools/>

———, 'Navigating the Ethics of Citizen Video: The Case of a Sexual Assault in Egypt', *Arab Media & Society*, 19 (2014), 1–7

———, 'When YouTube Videos Expose Crimes That Go Unpunished', *PBS Mediashift*, 24 February 2014 <http://www.pbs.org/mediashift/2014/02/when-youtube-videos-expose-crimes-that-go-unpunished/>

———, 'Will the Syrian Hero Boy Make Us Question Everything We See? (and Why Don't We Do That Already?)', *WITNESS Blog*, 20 November 2014 <http://blog.witness.org/2014/11/syrian-hero-boy/>

Bair, Madeleine, and Vienna Maglio, 'Photo, Video Verification Has Growing Role in Venezuela Protests', *WITNESS Blog*, 11 April 2014 <http://blog.witness.org/2014/04/growing-role-of-image-verification-in-venezuelas-protests/>

Baker, Vicky, 'Syria's Inside Track: Mapping Citizen Reporting', *Index on Censorship*, 43 (2014), 93–95 <http://dx.doi.org/10.1177/0306422014535688>

Barot, Trushar, 'Verifying Images', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 33–44 <verificationhandbook.com/book/chapter4.php>

BBC Academy, 'Social Media Verification: UGC Hub', *BBC Academy*, 2015
    <http://www.bbc.co.uk/academy/journalism/skills/social-
    media/article/art20130702112133524>

BBC News, 'Met Officers to Trial Body Cameras', *BBC News London*, 8 May 2014
    <www.bbc.co.uk/news/uk-england-london-27313500>

BBC Trending, '"I Am Tired": The Politics of Mexico's #Yamecanse Hashtag', *BBC Trending*, 9
    December 2014 <www.bbc.co.uk/news/blogs-trending-30294010>

Bellingcat, 'Home', *Bellingcat: By and for Citizen Investigative Journalists*, 2015
    <https://www.bellingcat.com>

Benetech, *Martus: Helping Human Rights Advocates Protect, Manage, and Effectively Utilize
    Information* (Benetech, n.d.) <www.martus.org/resources/Martus-Intro-Presentation-
    v50.pdf>

Booth, Liza, 'Can Technology Catch Criminals in Brazil?', *SmartPlanet*, 2014
    <www.smartplanet.com/blog/global-observer/can-technology-catch-criminals-in-brazil/>

Browne, Malachy, 'Verifying Video', in *Verification Handbook: An Ultimate Guideline on Digital Age
    Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands:
    European Journalism Centre, 2014), pp. 45–67
    <verificationhandbook.com/book/chapter5.php>

Brown, L. David, *Creating Credibility* (Sterling, VA: Kumarian Press, Inc., 2008)

Brysk, Alison, *The Politics of Human Rights in Argentina: Protest, Change, and Democratization*
    (Stanford, CA: Stanford University Press, 1994)

Byrne, Ciara, 'Welcome To PeaceTech, The Movement To Use Technology To End Violent Conflict And
    Extremism', *Fast Company*, 11 August 2015
    <http://www.fastcoexist.com/3047534/welcome-to-peacetech-the-movement-to-use-
    technology-to-end-violent-conflict-and-extremism>

Caja Madrid Obra Social, 'Capítulo 1', *La Aventura Universal de Los Derechos Humanos: Misión
    Interplanetaria*, n.d. <www.aventurauniversal.com/juego1.asp>

———, 'Padres Y Tutores', *La Aventura Universal de Los Derechos Humanos: Misión Interplanetaria*,
    n.d. <www.aventurauniversal.com/tutores.asp>

Clark, Ann Marie, *Diplomacy of Conscience: Amnesty International and Changing Human Rights Norms*
    (Princeton, NJ: Princeton University Press, 2001)

CrisisNET, 'Frequently Asked Questions', *CrisisNET*, 2014 <blog.crisis.net/frequently-asked-
    questions/>

Crowe, Anna, Sarah Lee, and Mark Verstraete, *Securing Safe Spaces Online: Encryption, Anonymity,
    and Human Rights* (Privacy International, 2015)
    <https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20O
    nline_0.pdf>

Daly, Emma, 'Why Tech Is a Double-Edged Sword for Human Rights', *Human Rights Watch*, 6 January
    2014 <www.hrw.org/news/2014/01/06/why-tech-double-edged-sword-human-rights>

Detekt, 'Intentions and Methods', *Detekt: Resist Surveillance*, n.d.
    <https://resistsurveillance.org/intentions.html>

Dewey, Caitlin, '#Bringbackourgirls, #Kony2012, and the Complete, Divisive History of "Hashtag
    Activism"', *The Washington Post*, 8 May 2014 <www.washingtonpost.com/news/the-
    intersect/wp/2014/05/08/bringbackourgirls-kony2012-and-the-complete-divisive-history-of-
    hashtag-activism/>

Diakopoulos, Nicholas, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes* (New
    York, NY: Columbia Journalism School Tow Center for Digital Journalism, 2013)
    <http://www.nickdiakopoulos.com/wp-content/uploads/2011/07/Algorithmic-
    Accountability-Reporting_final.pdf>

Edwards, Scott, and Christoph Koettl, 'The Amnesty Crowd: Mapping Saudi Arabia', *Ushahidi*, 20 June
    2011 <www.ushahidi.com/2011/06/20/amnesty-crowd/>

Efron, Sonni, 'Meet the Hacktivist Who Wants to Warn Syrians About Incoming Missiles', *The Atlantic*, 2 July 2013 <www.theatlantic.com/international/archive/2013/07/meet-the-hacktivist-who-wants-to-warn-syrians-about-incoming-missiles/277461/>

Elsayed-Ali, Sherif, 'The UK Government Spied on Us and We Won't Take It Lying Down', *Amnesty International*, 2 July 2015 <https://www.amnesty.org/en/latest/news/2015/07/the-uk-government-spied-on-us-and-we-wont-take-it-lying-down/>

eyeWitness to atrocities, 'About', *eyeWitness to Atrocities*, 2015 <http://www.eyewitnessproject.org/>

First Draft News, 'About', *First Draft News*, 2015 <https://medium.com/1st-draft/about>

Freedom House, *Freedom of the Net: China* (Freedom House, 2014) <freedomhouse.org/report/freedom-net/2014/china>

Front Line Defenders, *Front Line Defenders Annual Report 2015: Human Rights Defenders in the Balance* (Front Line Defenders, 13 January 2015) <www.frontlinedefenders.org/2015-Annual-Report>

Gandy, Oscar H., *Beyond Agenda Setting: Information Subsidies and Public Policy* (Norwood, NJ: Ablex Pub. Co., 1982)

Gibelman, Margaret, and Sheldon R. Gelman, 'A Loss of Credibility: Patterns of Wrongdoing Among Nongovernmental Organizations', *Voluntas: International Journal of Voluntary and Nonprofit Organizations*, 15 (2004), 355–81 <http://dx.doi.org/10.1007/s11266-004-1237-7>

Gladwell, Malcolm, 'Small Change: Why the Revolution Will Not Be Tweeted', *The New Yorker*, 4 October 2010 <www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell>

Greenhill, Kelly M., 'Nigeria's Countless Casualties: The Politics of Counting Boko Haram's Victims', *Foreign Affairs*, 9 February 2015 <www.foreignaffairs.com/articles/africa/2015-02-09/nigerias-countless-casualties>

Gregory, Sam, 'Co-Presence: A New Way to Bring People Together for Human Rights Activism', *WITNESS Blog*, 23 September 2013 <blog.witness.org/2013/09/co-presence-for-human-rights/>

———, 'How An Eyewitness Mode Helps Activists (and Others) Be Trusted', *WITNESS Blog*, 3 March 2014 <blog.witness.org/2014/03/eyewitness-mode-helps-activists/>

———, 'How We Can Use Livestreaming Apps to Promote Justice', *WIRED*, 10 May 2015 <www.wired.com/2015/05/can-use-livestreaming-apps-promote-justice/>

———, 'How We Can Use Livestreaming Apps to Promote Justice', *WIRED*, 2015 <http://www.wired.com/2015/05/can-use-livestreaming-apps-promote-justice/> [accessed 13 May 2015]

———, 'Images of Horror: Whose Roles and What Responsibilities?', *WITNESS Blog*, 18 September 2014 <blog.witness.org/2014/09/sharing-images-horror-roles-responsibilities/>

———, 'Visual Anonymity and YouTube's New Blurring Tool', *WITNESS Blog*, July 2012 <blog.witness.org/2012/07/visual-anonymity-and-youtubes-new-blurring-tool/>

Grupo Mood C.A, 'FotoAhora', *App Store*, 2014 <itunes.apple.com/us/app/fotoahora/id824442402?l=es>

Gunkel, David J., 'Second Thoughts: Toward a Critique of the Digital Divide', *New Media & Society*, 5 (2003), 499–522 <http://dx.doi.org/10.1177/146144480354003>

Guo, Chao, and Gregory D. Saxton, 'Tweeting Social Change How Social Media Are Changing Nonprofit Advocacy', *Nonprofit and Voluntary Sector Quarterly*, 43 (2014), 57–79 <http://dx.doi.org/10.1177/0899764012471585>

Gupta, Aditi, Ponnurangam Kumaraguru, Carlos Castillo, and Patrick Meier, 'TweetCred: A Real-Time Web-Based System for Assessing Credibility of Content on Twitter', in *Proceedings of Social Informatics (SocInfo 2014)*, 2014 <arxiv.org/abs/1405.5490>

Hankey, Stephanie, and Daniel Ó Clunaigh, 'Rethinking Risk and Security of Human Rights Defenders in the Digital Age', *Journal of Human Rights Practice*, 5 (2013), 535–47 <http://dx.doi.org/10.1093/jhuman/hut023>

Harvard Humanitarian Inititative, 'The Signal Program on Human Security and Technology', *Harvard Humanitarian Initiative*, 2013 <hhi.harvard.edu/programs-and-research/crisis-mapping-and-early-warning/signal-program>

Herman, Johanna, 'Hashtags and Human Rights: Activism in the Age of Twitter', *Carnegie Council for Ethics in International Affairs*, 2014 <www.carnegiecouncil.org/publications/ethics_online/0099>

Heyns, Christof, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns: Addendum*, Human Rights Council 17th Session (United Nations Office of the High Commissioner for Human Rights, 27 May 2011) <www.ohchr.org/Documents/Issues/Executions/A-HRC-17-28-Add1.pdf>

———, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Christof Heyns: Use of Information and Communications Technologies to Secure the Right to Life*, Human Rights Council 29th Session (United Nations Office of the High Commissioner for Human Rights, 24 April 2015) <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>

Himelfarb, Sheldon, 'Can Big Data Stop Wars Before They Happen?', *United States Institute of Peace*, 2014 <www.usip.org/publications/can-big-data-stop-wars-they-happen>

Himelfarb, Sheldon, and Anand Varghese, 'Peace, Inc.', *Foreign Policy*, 2015 <foreignpolicy.com/2015/01/27/peace-inc-tech-government-industry-defense-funding/>

Hindman, Matthew, *The Myth of Digital Democracy* (Princeton, NJ: Princeton University Press, 2010)

Howe, Jeff, 'Crowdsourcing: A Definition', *Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*, 2006 <crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html>

Human Rights Data Analysis Group, 'Core Concepts', *Human Rights Data Analysis Group*, 2015 <hrdag.org/coreconcepts/>

HURIDOCS, 'OpenEvsys – for Documenting Violations', *HURIDOCS*, 2015 <https://www.huridocs.org/openevsys/>

———, 'Research & Development', *HURIDOCS*, 2015 <https://www.huridocs.org/research-development/>

Igarapé Institute, 'Smart Policing', *Igarapé Institute: Progressive Alternatives for Security and Development*, n.d. <en.igarape.org.br/smart-policing/>

InformaCam, 'InformaCam - Secure & Verified Mobile Media', *InformaCam*, n.d. <guardianproject.info/informa/>

International Federation for Human Rights, 'Thunderclap: Free Syria's Silenced Voices', *Thunderclap*, 2014 <www.thunderclap.it/projects/9773-free-syria-s-silenced-voices?locale=en>

Karpf, David, 'Online Political Mobilization from the Advocacy Group's Perspective: Looking Beyond Clicktivism', *Policy & Internet*, 2 (2010), 7–41

———, *The MoveOn Effect: The Unexpected Transformation of American Political Advocacy* (New York, NY: Oxford University Press, 2012)

Kaye, David, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye*, Human Rights Council 29th Session (United Nations Office of the High Commissioner for Human Rights, 22 May 2015) <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>

Kayyali, Nadia, 'Want to Record The Cops? Know Your Rights', *Electronic Frontier Foundation*, 2015 <https://www.eff.org/deeplinks/2015/04/want-record-cops-know-your-rights>

Kehl, Danielle, Andi Wilson, and Kevin Bankston, *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s* (Open Technology Institute, CyberSecurity Initiative, 2015) <https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/OTI_Crypto_Wars_History.abe6caa19cbc40de842e01c28a028418.pdf>

Kelly, Sanja, Madeleine Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, *Tightening the Net: Governments Expand Online Controls* (Freedom House, 2014) <www.freedomhouse.org/report/freedom-net/2014/tightening-net-governments>

Kilroy, Della, 'Citizen Video for Journalists: Verification', *WITNESS Blog*, 25 February 2013 <blog.witness.org/2013/02/citizen-video-for-journalists-verification/>

King, Dan, 'Using SwiftRiver to Find the Needle in the Social Media Haystack', *Ushahidi*, 2014 <www.ushahidi.com/2014/12/09/using-swiftriver-find-needle-social-media-haystack-2/>

King, Gary, Jennifer Pan, and Margaret Roberts, 'Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation', *Science*, 345 (2014), 1–10

Koettl, Christoph, 'About & FAQ', *Citizen Evidence Lab*, 2014 <www.citizenevidence.org/about/>

———, 'Human Rights Citizen Video Assessment Tool', *Citizen Evidence Lab*, 2014 <fluidsurveys.com/s/citizenvideo-stress-test/>

———, 'The Story behind the Boko Haram Satellite Images', *Amnesty International UK / Blogs: Into the Ether*, 2015 <www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satellite-images>

———, '"The YouTube War": Citizen Videos Revolutionize Human Rights Monitoring in Syria', *PBS*, 18 February 2014 <www.pbs.org/mediashift/2014/02/the-youtube-war-citizen-videos-revolutionize-human-rights-monitoring-in-syria/>

———, 'YouTube Data Viewer', *Citizen Evidence Lab*, 2014 <citizenevidence.org/2014/07/01/youtube-dataviewer/>

Landman, Todd, 'Resources', *Human Rights Atlas*, 2015 <www.humanrightsatlas.org/resources/>

Land, Molly, 'Networked Activism', *Harvard Human Rights Journal*, 22 (2009), 205–43

———, 'Participatory Fact-Finding: Developing New Directions for Human Rights Investigations Through New Technologies', in *The Future of Human Rights Fact-Finding*, ed. by Philip Alston and Sarah Knuckey (Oxford, UK: Oxford University Press, Forthcoming)

———, 'Peer Producing Human Rights', *Alberta Law Review*, 46 (2009), 1115–39

Land, Molly, Patrick Meier, Mark Belinsky, and Emily Jacobi, *#ICT4HR: Information and Communication Technologies for Human Rights* (Rochester, NY: Social Science Research Network, 20 November 2012) <http://papers.ssrn.com/abstract=2178484>

Larsen, Rebekah, and Ella McPherson, 'Encryption, Anonymity & Human Rights Workshop', *Centre of Governance and Human Rights, University of Cambridge*, 2015 <http://www.cghr.polis.cam.ac.uk/research-themes/human-rights-in-the-digital-age-1/encryption-and-human-rights-workshop>

Lewsey, Fred, 'First Scientific Report Shows Police Body-Worn-Cameras Can Prevent Unacceptable Use-of-Force', *University of Cambridge*, 23 December 2014 <http://www.cam.ac.uk/research/news/first-scientific-report-shows-police-body-worn-cameras-can-prevent-unacceptable-use-of-force>

Loken, Meredith, '#BringBackOurGirls and the Invisibility of Imperialism', *Feminist Media Studies*, 14 (2014), 1100–1101 <http://dx.doi.org/10.1080/14680777.2014.975442>

Lorinc, John, 'New Era of Policing: Will the Benefits of Body-Worn Cameras Outweigh the Privacy Issues?', *The Globe and Mail*, 21 November 2014 <http://www.theglobeandmail.com/news/national/new-era-of-policing-will-the-benefits-of-body-worn-cameras-outweigh-the-privacy-issues/article21698547/>

Lovejoy, Kristen, and Gregory D. Saxton, 'Information, Community, and Action: How Nonprofit Organizations Use Social Media', *Journal of Computer-Mediated Communication*, 17 (2012), 337–53 <http://dx.doi.org/10.1111/j.1083-6101.2012.01576.x>

Luckerson, Victor, 'Here's How Your Facebook News Feed Actually Works', *Time*, 9 July 2015 <http://time.com/3950525/facebook-news-feed-algorithm/>

Lynch, Marc, Deen Freelon, and Sean Aday, *Syria's Socially Mediated Civil War* (Washington, D.C.: United States Institute of Peace, 13 January 2014) <http://www.usip.org/publications/syria-s-socially-mediated-civil-war>

Malsin, Jared, 'Western Media: Stop Ignoring the Central African Republic Crisis', *Columbia Journalism Review*, 13 October 2014 <http://www.cjr.org/behind_the_news/western_media_stop_ignoring_th.php>

Manske, Jiva, 'Case Studies: Concrete Examples of Compelling and Strategic Use of Social Media', *New Tactics in Human Rights*, 2013 <https://www.newtactics.org/comment/6124>

McKenzie, David J., *Youth, ICTs, and Development* (Washington, DC: World Bank, 2007) <http://documents.worldbank.org/curated/en/2007/03/7458887/youth-icts-development>

McPherson, Ella, 'Advocacy Organizations' Evaluation of Social Media Information for NGO Journalism: The Evidence and Engagement Models', *American Behavioral Scientist*, 59 (2014), 124–48 <http://dx.doi.org/10.1177/0002764214540508>

———, 'Digital Human Rights Reporting by Civilian Witnesses: Surmounting the Verification Barrier', in *Produsing Theory in a Digital World 2.0: The Intersection of Audiences and Production in Contemporary Theory*, ed. by Rebecca Ann Lind (New York, NY: Peter Lang Publishing, 2015), II, 193–209

———, 'Source Credibility as "Information Subsidy": Strategies for Successful NGO Journalism at Mexican Human Rights NGOs' (working paper, 2015) <https://www.academia.edu/8157551/Credibility_as_Information_Subsidy_NGO_Journalism_at_Human_Rights_Organizations_in_Mexico>

McPherson, Ella, and Mónica Moreno Figueroa, 'Smoke, Mirrors and Murder: The Disappearance and Killing of Student Protesters in Mexico', *Red Pepper*, March 2015, pp. 36–37

Meier, Patrick, 'Combining Crowdsourced Satellite Imagery Analysis with Crisis Reporting: An Update on Syria', *iRevolutions*, 19 September 2011 <http://irevolution.net/2011/09/19/crowdsourcing-update-on-syria/>

———, 'From Crowdsourcing Crisis Information to Crowdseeding Conflict Zones (Updated)', *iRevolutions*, 10 July 2012 <http://irevolution.net/2012/07/10/crowdsourcing-to-crowdseeding/>

———, 'How to Verify Social Media Content: Some Tips and Tricks on Information Forensics', *iRevolutions*, 21 June 2011 <http://irevolution.net/2011/06/21/information-forensics/>

———, 'PeaceTXT Kenya: Since Wars Begin in the Minds of Men', *PopTech*, 4 March 2013 <http://poptech.org/blog/peacetxt_kenya_since_wars_begin_in_the_minds_of_men>

———, 'Will Using "Live" Satellite Imagery to Prevent War in the Sudan Actually Work?', *iRevolutions*, 30 December 2010 <http://irevolution.net/2010/12/30/sat-sentinel-project/>

Moore, Will, 'About', *Citizen Media Evidence Partnership (C-MEP)*, 2014 <http://c-mep.org/home/about/>

Morgan, Jonathon, 'Syrian Social Media, Journalists' Secret Weapon in the Crisis Data Revolution', *CrisisNET*, 3 June 2014 <http://blog.crisis.net/syrian-social-media-journalists-secret-weapon-in-the-crisis-data-revolution/>

Mosco, Vincent, *The Political Economy of Communication*, 2nd edn (London, UK: SAGE Publications Ltd, 2009)

Muggah, Robert, 'Why Police Body Cameras Are Taking Off, Even After Eric Garner's Death', *IPI Global Observatory*, 11 December 2014 <http://theglobalobservatory.org/2014/12/police-body-cameras-eric-garner/>

Murphy, Jim, 'Top 30 Human Rights Tweets of 2014', *Huffington Post*, 22 December 2014 <http://www.huffingtonpost.com/jim-murphy/top-30-human-rights-tweet_b_6366690.html>

Naroditskiy, Victor, 'Veri.ly - Getting the Facts Straight During Humanitarian Disasters', *Software Sustainability Institute*, 2014 <http://www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitarian-disasters>

Neu, Christopher, 'Mobile Applications for Atrocity Prevention Require Mobile Students', *TechChange*, 2013 <http://techchange.org/2013/02/19/mobile-applications-for-atrocity-prevention-require-mobile-students/>

New Tactics in Human Rights, 'Incorporating Social Media into Your Human Rights Campaigning', *New Tactics in Human Rights*, 2013 <https://www.newtactics.org/conversation/incorporating-social-media-your-human-rights-campaigning>

———, 'Staying Safe: Security Resources for Human Rights Defenders', *New Tactics in Human Rights*, 2010 <https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders>

———, 'Using Video for Documentation and Evidence', *New Tactics in Human Rights*, 2014 <https://www.newtactics.org/conversation/using-video-documentation-and-evidence>

Norton, Tim, *Social Media Strategies for Advocacy and Targeted Communications* (Internews, 2013) <http://tim.anewleaf.com.au/files/2013/03/Social-Media-for-Advocacy-v1.pdf>

Nuwer, Rachel, 'The Fake Story of a Blond Child Bride Made This the Most Visited Blog in Norway', *Smithsonian*, 8 October 2014 <http://www.smithsonianmag.com/smart-news/fake-story-blond-child-bride-made-most-visited-blog-norway-180952977/>

Obar, Jonathan A, Paul Zube, and Cliff Lampe, 'Advocacy 2.0: An Analysis of How Advocacy Groups in the United States Perceive and Use Social Media as Tools for Facilitating Civic Engagement and Collective Action', *Journal of Information Policy*, 2 (2012), 1–25

O'Carroll, Tanya, 'More than an App: The Panic Button, One Year on', *Amnesty International*, 22 July 2015 <https://www.amnesty.org/en/latest/campaigns/2015/07/panic-button-one-year-on/>

Office of the Press Secretary, 'Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013', *The White House*, 2013 <http://www.whitehouse.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21>

Padania, Sameer, 'Advocacy's Long and Winding Road', *Sameer Padania*, 2012 <http://blog.sameerpadania.com/2012/07/19/youtube-witness-face-blurring-advocacy/>

———, 'The Ethics of Face Recognition Technology', *WITNESS Blog*, 7 March 2012 <http://blog.witness.org/2012/03/the-ethics-of-face-recognition-technology/>

Padania, Sameer, Sam Gregory, Yvette Alberdingk-Thijm, and Bryan Nunez, *Cameras Everywhere: Current Challenges and Opportunities at the Intersection of Human Rights, Video and Technology* (Brooklyn, NY: Witness, 2011) <http://www.ohchr.org/Documents/Issues/Opinion/Communications/Witness_1.pdf>

Panic Button, 'Managing Your Risks', *Panic Button*, n.d. <https://panicbutton.io/help/help-risk.html>

pipl, 'Welcome to the Deep Web', *Pipl*, 2015 <https://pipl.com/help/deep-web/>

Pizzi, Michael, 'The Syrian Opposition Is Disappearing from Facebook', *The Atlantic*, 4 February 2014 <http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562/>

Prakash, Aseem, and Mary Kay Gugerty, 'Advocacy Organizations and Collective Action: An Introduction', in *Advocacy Organizations and Collective Action*, ed. by Aseem Prakash and Mary Kay Gugerty (Cambridge, UK: Cambridge University Press, 2010), pp. 1–28

Purdon, Lucy, *Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections, Case Study: Safaricom* (Institute for Human Rights and Business, 2013) <http://www.ihrb.org/pdf/DD-Safaricom-Case-Study.pdf>

Quinn, Timothy, 'Introducing Hatebase: The World's Largest Online Database of Hate Speech', *The Sentinel Project*, 2013 <https://thesentinelproject.org/2013/03/25/introducing-hatebase-the-worlds-largest-online-database-of-hate-speech/>

———, 'Meet HateBrain, the Automated Social Media Monitoring Engine at the Heart of Hatebase', *The Sentinel Project*, 2013 <https://thesentinelproject.org/2013/07/23/meet-hatebrain-the-automated-social-media-monitoring-engine-at-the-heart-of-hatebase/>

Ratner, Steven R., 'The Political Dimension of International Human Rights Fact-Finding', in *Proceedings of the Annual Meeting (American Society of International Law)*, 2013, CVII, 70–72

Raymond, Nathaniel A., Benjamin I. Davies, Brittany L. Card, Ziad Al Achkar, and Isaac L. Baker, 'While We Watched: Assessing the Impact of the Satellite Sentinel Project', *Georgetown Journal of*
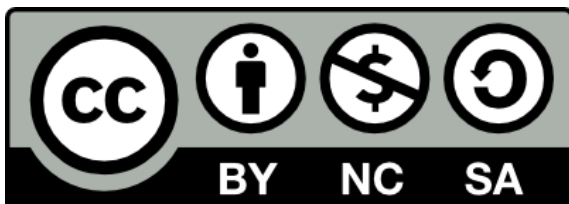
International Affairs, 26 July 2013 <http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/>

Robertson, Andrew, and Steve Olson, *Sensing and Shaping Emerging Conflicts: Report of a Workshop by the National Academy of Engineering and United States Institute of Peace Roundtable on Technology, Science, and Peacebuilding* (Washington, D.C.: The National Academies Press, 2013) <http://www.usip.org/sites/default/files/Sensing_And_Shaping_Emerging_Conflicts.pdf>

Romero, Cynthia, *What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World* (USAID, 2014) <https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf>

De Rosa, Anthony, 'Using Social Media as a Police Scanner', *Verification Handbook*, 2014 <verificationhandbook.com/book/chapter2.1.php>

Rutkin, Aviva, 'Facebook Can Recognise You in Photos Even If You're Not Looking', *New Scientist*, 22 June 2015 <https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking>

Saber, Dima, *Checkdesk: Sorting, Developing & Disseminating Citizen Reporting in the MENA Region* (Birmingham City University and The University of Manchester, 2013) <https://www.academia.edu/8269524/Checkdesk_Sorting_Developing_and_Disseminating_Citizen_Reporting_in_the_MENA_Region>

Saleh, Nivien, 'Egypt's Digital Activism and the Dictator's Dilemma: An Evaluation', *Telecommunications Policy*, 36 (2012), 476–83 <http://dx.doi.org/10.1016/j.telpol.2012.04.001>

Sanburn, Josh, 'Police Eye Google Glass as Surveillance Tool', *Time*, 17 February 2014 <http://nation.time.com/2014/02/17/police-eye-google-glass-as-surveillance-tool/>

Satterthwaite, Margaret, 'Finding, Verifying, and Curating Human Rights Facts', in *Proceedings of the Annual Meeting (American Society of International Law)*, 2013, CVII, 62–65

Satterthwaite, Margaret L., and Justin Simeone, *An Emerging Fact-Finding Discipline? A Conceptual Roadmap for Social Science Methods in Human Rights Advocacy*, Public Law & Legal Theory Research Paper Series (New York, NY: New York University School of Law, 2014) <http://papers.ssrn.com/abstract=2468261>

Saunders, Alphea, 'Body Cameras for Policemen', *Jamaica Information Service*, 2014 <http://jis.gov.jm/body-cameras-policemen/>

Saxton, Gregory D., Jerome N. Niyirora, Chao Guo, and Richard D. Waters, '#AdvocatingForChange: The Strategic Use of Hashtags in Social Media Advocacy', *Advances in Social Work*, 16 (2015), 154–69

Schudson, Michael, 'The Sociology of News Production Revisited (Again)', in *Mass Media and Society*, ed. by James Curran and Michael Gurevitch, 3rd edn (London, UK: Arnold, 2000), pp. 175–200

De Schutter, Olivier, 'International Human Rights', *edX*, 2015 <www.edx.org/course/international-human-rights-louvainx-louv2x>

Scott-Railton, John, and Morgan Marquis-Boire, 'A Call to Harm: New Malware Attacks Target the Syrian Opposition', *The Citizen Lab*, 21 June 2013 <https://citizenlab.org/2013/06/a-call-to-harm/>

Segun, Mausi, 'Dispatches: What Really Happened in Baga, Nigeria?', *Human Rights Watch*, 14 January 2015 <http://www.hrw.org/news/2015/01/14/dispatches-what-really-happened-baga-nigeria>

Setrakian, Lara, 'Citizen Video for Journalists: Contextualization', *WITNESS Blog*, 1 April 2013 <http://blog.witness.org/2013/04/citizen-video-for-journalists-contextualization/>

Sharp, Dustin N., 'Human Rights Fact-Finding and the Reproduction of Hierarchies', in *Human Rights Fact-Finding in the 21st Century*, ed. by Philip Alston and Sarah Knuckey (Oxford, UK: Oxford University Press, Forthcoming) <http://papers.ssrn.com/abstract=2341186>

Shirky, Clay, 'The Political Power of Social Media', *Foreign Affairs*, February 2011
    <http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-
    media>

Silent Lens, 'Silent Lens', *Silent Lens*, n.d. <http://silentlens.com>

Silverman, Craig, ed., *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for
    Emergency Coverage* (Maastricht, the Netherlands: European Journalism Centre, 2014)

———. , ed., *Verification Handbook for Investigative Reporting: A Guide to Online Search and
    Research Techniques for Using UGC and Open Source Information in Investigations*
    (Maastricht, the Netherlands: European Journalism Centre, 2015)
    <http://verificationhandbook.com/downloads/verification.handbook.2.pdf>

———. , ed., 'Verification Tools', in *Verification Handbook: An Ultimate Guideline on Digital Age
    Sourcing for Emergency Coverage* (Maastricht, the Netherlands: European Journalism Centre,
    2014), pp. 108–10 <http://verificationhandbook.com/book/chapter10.php>

Silverman, Craig, and Rina Tsubaki, 'When Emergency News Breaks', in *Verification Handbook: An
    Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman
    (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 5–12
    <http://verificationhandbook.com/book/chapter1.php>

Singer, Natasha, 'Never Forgetting a Face', *The New York Times*, 17 May 2014
    <http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html>

Slater, Don, *New Media, Development and Globalization: Making Connections in the Global South*
    (Cambridge, UK: Polity, 2014)

Smith, David James, 'Videre: The Secretive Group on a Mission to Film Human-Rights Abuses', *Wired
    UK*, 29 August 2013 <http://www.wired.co.uk/magazine/archive/2013/09/features/videre>

Sniderman, Andrew Stobo, and Mark Hanis, 'Drones for Human Rights', *The New York Times*, 30
    January 2012 <www.nytimes.com/2012/01/31/opinion/drones-for-human-rights.html>

Standby Task Force, 'What We Do', *Standby Task Force*, n.d. <http://blog.standbytaskforce.com/our-
    model/what-we-do/>

Stearns, Josh, 'Verification Junkie', *Verification Junkie*, 2015 <http://verificationjunkie.com/?og=1>

Stein Kerr, Sarah, 'Drones for Good? The Basic Human Rights Considerations', *WITNESS Blog*,
    November 2013 <https://blog.witness.org/2013/11/drones-for-good-the-basic-human-
    rights-considerations/>

Stockley, Bracken, 'Public Support for Police Body Cameras – but Who Controls On/off Switch?', *The
    Justice Gap*, 2014 <http://thejusticegap.com/2014/03/body-worn-video-cameras-scrutiny/>

Storyful, 'Storyful Blog', *Storyful*, 2015 <http://blog.storyful.com/>

Strochlic, Nina, 'Can This Bracelet Save Your Life', *PFO Tech*, n.d.
    <http://www.pfotech.com/2013/04/06/can-bracelet-save-life-newsweek/>

Sutherlin, Gwyneth, 'Letters: The Problem with Mapping Hate Speech', *Foreign Policy*, 11 April 2013
    <http://foreignpolicy.com/2013/04/11/letters-the-problem-with-mapping-hate-speech/>

Syria Tracker, 'Submit a Report', *Syria Tracker*, n.d.
    <https://syriatracker.crowdmap.com/reports/submit>

The Guardian Project, 'CameraV App and the InformaCam System', *CameraV*, 2015
    <https://guardianproject.github.io/informacam-guide/en/InformacamGuide.html>

———, 'CameraV: Secure Verifiable Photo & Video Camera', *The Guardian Project*, 2015
    <https://guardianproject.info/apps/camerav/>

———, 'ObscuraCam: Secure Smart Camera', *The Guardian Project*, 2015
    <https://guardianproject.info/apps/obscuracam/>

The Rashomon Project, 'About Rashomon', *The Rashomon Project*, n.d.
    <http://rieff.ieor.berkeley.edu/rashomon/about-rashomon/>

The Whistle, 'About', *The Whistle*, 2015 <http://www.thewhistle.org>

Thompson, Nicholas, 'Why Did Syria Shut Down the Internet?', *The New Yorker*, 2013
    <http://www.newyorker.com/news/daily-comment/why-did-syria-shut-down-the-internet>

Thrall, A. Trevor, Dominik Stecula, and Diana Sweet, 'May We Have Your Attention Please? Human-Rights NGOs and the Problem of Global Communication', *The International Journal of Press/Politics*, 19 (2014), 135–59 <http://dx.doi.org/10.1177/1940161213519132>

Thunderclap, 'Bringing the Thunder', *Thunderclap*, 2012 <https://www.thunderclap.it/casestudies>

Toor, Amar, 'Camera Cops: Digital Spying in Rio's Most Dangerous Slums', *The Verge*, 21 October 2013 <http://www.theverge.com/2013/10/21/4861176/smart-policing-android-app-igarape-google-ideas-police-surveillance-rio-favelas>

Tor, 'Tor: Overview', *Tor*, n.d. <https://www.torproject.org/about/overview.html.en>

Treem, Jeffrey W., and Paul M. Leonardi, 'Social Media Use in Organizations: Exploring the Affordances of Visibility, Editability, Persistence, and Association', *Communication Yearbook*, 36 (2012), 143–89

Tufekci, Zeynep, 'What Happens to #Ferguson Affects Ferguson', *Medium*, 14 August 2014 <https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0>

United Nations Human Rights, 'UN Rights Chief Zeid Condemns Attacks on Human Rights Defenders in Libya', *United Nations Human Rights: Office of the High Commissioner for Human Rights*, 14 October 2014 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15168>

United Nations Office for the Coordination of Humanitarian Affairs, *Humanitarianism in the Network Age*, OCHA Policy and Studies Series (New York, NY: United Nations Office for the Coordination of Humanitarian Affairs, 2013) <https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf>

Ushahidi, 'Ushahidi's Mission', *Ushahidi*, 2015 <http://www.ushahidi.com/mission/>

Vale, Paul, 'Russia Threatens To Block Facebook, Google And Twitter', *The Huffington Post UK*, 22 May 2015 <http://www.huffingtonpost.co.uk/2015/05/22/russia-threatens-to-ban-facebook-google-and-twitter-unless-companies-turn-over-user-data_n_7423550.html>

Veri.ly, 'Is This Highgate Cemetery?', *Veri.ly*, 2014 <https://veri.ly/crisis/3/question/81-is-this-highgate-cemetery>

Vie, Stephanie, 'In Defense of "slacktivism": The Human Rights Campaign Facebook Logo as Digital Activism', *First Monday*, 19 (2014) <http://firstmonday.org/ojs/index.php/fm/article/view/4961>

Waldman, Annie, 'Death by Cop: Invisible Numbers', *BBC News*, 27 August 2014 <http://www.bbc.co.uk/news/blogs-echochambers-28946204>

Wang, Ben Yunmo, Nathaniel A. Raymond, Gabrielle Gould, and Isaac Baker, 'Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities', *Stability: International Journal of Security & Development*, 2 (2013), 53 <http://dx.doi.org/10.5334/sta.cn>

Wardle, Claire, 'Verifying User-Generated Content', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European Journalism Centre, 2014), pp. 24–33 <http://verificationhandbook.com/downloads/verification.handbook.pdf>

Washington Office on Latin America, 'Too Early to Close the Ayotzinapa Case: Mexican Government's Actions Undermine Rule of Law', *Washington Office on Latin America*, 2015 <http://www.wola.org/news/too_early_to_close_the_ayotzinapa_case>

Watson, Tom, 'Inside Amnesty's Panic Button App: Simple Technology, Serious Impact For Activists', *Forbes*, 23 June 2014 <http://www.forbes.com/sites/tomwatson/2014/06/23/inside-amnestys-panic-button-app-simple-technology-serious-impact-for-activists/>

Whitten, Alma, and J. D. Tygar, 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0', in *Security and Usability: Designing Secure Systems That People Can Use*, ed. by Lorrie Cranor and Garfinkel Simson (Sebastopol, CA: O'Reilly Media, Inc., 2005), pp. 679–702

Van der Windt, Peter, 'Voix Des Kivus: A Crowd-Seeding System in DRC', *Ushahidi*, 16 May 2011
    <http://www.ushahidi.com/blog/2011/05/16/voix-des-kivus-a-crowd-seeding-system-in-
    drc/>

Witness, 'Activists' Guide to Archiving Video', *Witness*, 2013 <http://archiveguide.witness.org>

———, 'Appendix: "VISUALIZE JUSTICE: A Field Guide to Enhancing the Evidentiary Value of Video for
    Human Rights"', in *Verification Handbook: An Ultimate Guideline on Digital Age Sourcing for
    Emergency Coverage*, ed. by Craig Silverman (Maastricht, the Netherlands: European
    Journalism Centre, 2014), pp. 109–12
    <http://verificationhandbook.com/book/appendix.php>

———, 'Witness Media Lab Resources', *Witness Media Lab*, 2015
    <https://lab.witness.org/resources/>

Youmans, William Lafi, and Jillian C. York, 'Social Media and the Activist Toolkit: User Agreements,
    Corporate Interests, and the Information Infrastructure of Modern Social Movements',
    Journal of Communication, 62 (2012), 315–29 <http://dx.doi.org/10.1111/j.1460-
    2466.2012.01636.x>

Youth for Human Rights International, 'Youth for Human Rights Online Education App', *Youth for
    Human Rights Online Education*, 2015 <http://education.youthforhumanrights.org/edu-
    translated.html>

Youtube, 'Face Blurring: When Footage Requires Anonymity', *Official YouTube Blog*, 18 July 2012
    <http://youtube-global.blogspot.com/2012/07/face-blurring-when-footage-requires.html>

Zittrain, Jonathan, 'The Internet Creates a New Kind of Sweatshop', *Newsweek*, 7 December 2009
    <http://www.newsweek.com/internet-creates-new-kind-sweatshop-75751>