Chapter X
Using Information and Communication Technologies to Protect the Right to Life

A. Introduction

B. Use of ICTs for Protecting the Right to Life

1. Promotion and advocacy
2. Prevention and protection
3. Monitoring and fact-finding
4. Evaluating evidence collected using ICTs
5. Use of ICTs by human rights mechanisms

A. Introduction

Human rights monitoring methods have evolved significantly over time.[1] Factfinding is conducted by diverse actors, from directly affected individuals and communities, to local civil society groups, social movements, national and international NGOs, and intergovernmental organizations. As new technologies have developed, a wide range of actors, including citizen activists and direct witnesses to an abuse, have been able to gather, record, store, verify, and share information. Throughout their mandates, the Special Rapporteurs were able to benefit from the work of these factfinders. To do so, the Rapporteurs often had to evaluate claims made about unlawful killings that relied upon the use of new information communication technologies (ICTs).

In 2010, Special Rapporteur Alston discussed the benefits of embracing ICTs in human rights fact-finding.

> ***Report to the General Assembly (A/65/321, 23 August 2010, ¶¶3-5)***
>
> 3. Even in situations involving large-scale extrajudicial executions, major difficulties arise in efforts to gather accurate information on the events in question. This is partly because some Governments are becoming both more determined and more skilled in blocking access to information, but it is also because human rights groups, as a whole, have not yet moved in a sufficiently sustained or systematic fashion to take advantage of the enormous potential provided by new information and communication technologies to enhance their fact-finding capacities.
>
> 4. International human rights fact-finding currently relies heavily on witness testimony, usually gathered through lengthy in-person interviews by experienced investigators and advocates. International fact-finders spend weeks or months at a time investigating incidents and searching for witnesses, sometimes relying on trusted local organizations, media accounts, or word of mouth for contacts. The number of individual incidents that can be recorded depends in large part on the size of the fact-finding team, the amount of time its members can spend in-country, and the availability of funding. Fact-finding can be impeded or sometimes rendered impossible where investigators are unable, for security reasons or because of other obstacles, to access to meet with potential witnesses or examine the sites of alleged abuse. In such cases, grave abuses, including massacres, may be unknown to outsiders for months or longer, delaying potentially life-saving reporting and intervention.[2] In other cases, heavy reliance on witness testimony which is not supported by additional information of a more objective nature may leave findings open to challenge by Governments or alleged perpetrators. The long written reports that generally detail the results of a fact-finding mission may not make it easy to fully explain the complexities of a situation, or may fail to engage a broad audience.
>
> 5. New technologies offer a great many potential solutions to some of these problems, and offer significant improvements in existing fact-finding methodologies. Surprisingly, however, there remains an enormous gap between the human rights and information and communications technology fields. Little sustained work has been undertaken by the human rights community as a whole to apply existing technologies or to study their potential uses and problems, and far too little attention has been given to the research and development of information and communications technologies with human rights applications. As a result, the use of information and communications technologies in human rights work is only at a nascent stage.[3] Nevertheless [...] some efforts are

1 See generally, Philip Alston and Sarah Knuckey (eds.), *The Transformation of Human Rights Fact-Finding* (Oxford University Press, 2015).

2 See Report of the Special Rapporteur, Philip Alston, Mission to DRC, A/HRC/14/24/Add.3 14 June 2010, paras. 26-30 (describing massacres that took place in the Democratic Republic of the Congo in April and August 2009, but that were not reported until months later).

3 There is also a large gap between the humanitarian and information and communications technology (ICT) communities, but it is narrowing, particularly since the Haiti earthquake. See Diane Coyle and Patrick Meier, "New technologies in Emergencies and Conflicts: The Role of Information and Social Networks" (United Nations

already under way to exploit new technologies to increase public participation in the monitoring and reporting of abuses. Some may enable the reporting of abuses in real time, thereby increasing awareness of incidents and speeding up responsiveness and, potentially, prevention; some provide human rights investigators access to new types of data which may provide important supporting evidence of human rights abuses; and others present new advocacy opportunities.

In 2015, Special Rapporteur Heyns dedicated a thematic report to the Human Rights Council to exploring the use of ICTs to enhance protection of the right to life.

Report to the Human Rights Council (A/HRC/29/37, 24 April 2015, ¶¶35, 37-42)

35. Given that many of the norms of international law concerning the right to life have broadly been settled, the work relating to protecting this right often concerns disputed facts or even the availability of facts. Individuals commit violations of the right to life not because they believe it is justifiable, but because they believe they will not be called on to justify themselves. That places a premium on fact-finding and evidence.

[...]

37. It has become clear that information and communications technologies (ICTs)—the hardware and software that facilitate the production, transmission, reception, archiving and storage of information—can play an increasing role in the protection of all human rights, including the right to life. Information harnessed in this way can be used to secure accountability, but the technology can also ensure visibility or mobilise support for persons in immediate danger.

38. In his daily work of identifying and assessing claims about unlawful killings, the Special Rapporteur, like many others in the field, is increasingly dependent on information mediated through technology. See, for example, the use of video material taken with cell phones during the civil war in Sri Lanka to press both the State and the international community for fuller investigation of the widespread violations of many human rights, including the right to life, alleged to have occurred (A/HRC/17/28/Add.1). Similarly, in preparing the report to the Human Rights Council on the safety of journalists, it became clear how salient citizen journalists and civic media had become through their use of technology to highlight and document violations around the world (A/HRC/20/22 and Corr.1).

39. Increasing digital capacity is greatly enhancing the ability of ordinary people to participate in human rights monitoring. Digital ICTs create opportunities for pluralism that can democratise the process of human rights fact-finding, as well as offer mechanisms of social accountability that citizens can use to hold States and others to account.[4] Social media have created a wealth of opportunities for civilians to highlight human rights violations that they have witnessed, often unmediated by formal intergovernmental or non-governmental structures. This has far-reaching implications for the established power relations in human rights monitoring as there is a much wider community of human rights monitors at work than ever before. It also presents opportunities in contexts that might otherwise be closed to scrutiny. In circumstances where the physical presence of human rights investigators can be a challenge, the sensitive use of ICTs can help to avoid information austerity about situations that are of great interest to the human rights community.

Foundation-Vodafone Foundation Partnership, 2009); P.G. Greenough et al, "Applied Technologies in Humanitarian Assistance: Report of the 2009 Applied Technology Working Group", Prehospital and Disaster Medicine, 24 (2009); Hillary Rodham Clinton, United States Secretary of State, "Remarks on Internet Freedom" (21 January 2010).

4 Molly K. Land and others, *#ICT4HR: Information and Communication Technologies for Human Rights* (World Bank Institute, 2012).

> 40. However, the development of ICTs should not be viewed as an unqualified good in terms of the protection of human rights. Opportunities for States to carry out surveillance on and interfere in the work of civil society have multiplied in the digital space, and the Council should be vigilant concerning the dangers as well as the affordances of ICTs.[5] The use of technology by human rights activists and others can expose them to a range of risks, of which many may not be aware.
>
> 41. In order to fully realise the potential of ICTs for human rights work, it is necessary to address the issue of the digital divide in terms of both access and literacy. On the one hand, ICTs facilitate pluralism within human rights work, allowing amateurs to complement professionals; on the other hand, however, they can create new lines of inclusion and exclusion that often correspond with pre-existing barriers to access to resources and power, such as language, education, affluence or gender.[6] Moreover, in addition to providing opportunities to speak, pluralism is also about being heard. Being heard by human rights fact-finders may depend on one's ability to produce verifiable information, which can in turn be determined by one's digital literacy and digital footprint.[7] The greater availability of digital information on human rights violations in one context or region may lead to such violations being prioritised over more egregious but less visible violations elsewhere.
>
> 42. It is clear that, if used sensibly, ICTs can enhance the protection of human rights, including the right to life. Various parts of the wider United Nations system have been investing significant time and resources into accommodating the affordances of ICTs into their methods of work. The Office for the Coordination of Humanitarian Affairs and the Department of Peacekeeping Operations have been developing advanced techniques for crisis monitoring and mapping. The International Criminal Court has undertaken a review into the way it handles digital evidence. Nonetheless, it still seems that the full potential of these new tools has not been systematically investigated and internalised by the human rights community (see A/65/321, paras. 3–10).

At the time that this 2015 report was presented, Special Rapporteur Heyns also used a press release to amplify his recommendation to the Office of the High Commissioner for Human Rights and to other international human rights mechanisms to make greater use of ICTs to protect human rights:

> ***Press Release: New technologies—if used right—are vital tools in the fight against human rights violations (Geneva, 19 June 2015)***
>
> The United Nations Special Rapporteur on summary executions, Christof Heyns, has called on the UN system and other international human rights bodies to "catch up" with rapidly developing innovations in human rights fact-finding and investigations. "The digital age presents challenges that can only be met through the smart use of digital tools," he said.
>
> In his latest report to the Human Rights Council, Mr. Heyns highlighted that information and communication technologies (ICTs)—the hardware and software that produce and transmit information in the digital space—can play an increasing role in the protection of all human rights, including the right to life, by reinforcing the role of 'civilian witnesses' in documenting rights violations.
>
> "We have all seen how the actions of police officers and other who use excessive force are captured on cell phones and lead to action against the perpetrators. Billions of people around the world

5 The Special Rapporteur notes that, at its twenty-eighth session, the Human Rights Council decided to appoint a special rapporteur on the right to privacy in the digital age.

6 A. Trevor Thrall, Dominik Stecula and Diana Sweet, "May we have your attention please? Human rights NGOs and the problem of global communication", *International Journal of Press/Politics*, 19 (April 2014), pp. 135–59.

7 Ella McPherson, "Advocacy organizations' evaluation of social media information for NGO journalism: the evidence and engagement models", *American Behavioral Scientist*, 59 (July 2014), pp. 124–48.

carry a powerful weapon to capture such events in their pockets," the expert said. "The fact that this is well-known can be a significant deterrent to abuses."

The expert described in his report how various organizations are developing alert applications that journalists, human rights defenders and others can use to send an emergency message (along with GPS co-ordinates) to their friends and colleagues if they feel in immediate danger.

"New information tools can also empower human rights investigations and help to foster accountability where people have lost their lives or were seriously injured," the Special Rapporteur noted.

The use of other video technologies, ranging from CCTV cameras to body-worn "cop cams" can further contribute to filling information gaps. The use of resources such as satellite imagery to verify such videos, or sometime to show evidence of violations themselves, is also an important dimension.

However, despite the many advantages offered by ICTS for the protection of human rights, Mr. Heyns also warned that it will be short-sighted not to see the risks. "Those with the power to violate human rights can easily use peoples' emails and other communications to target them and also to violate their privacy," he said.

The human rights expert also noted that the fact that people can use social media to organise spontaneous protests can lead authorities to perceive a threat – and to over-react.

Moreover, there is a danger that what is not captured on video is not taken seriously. "We must guard against a mind-set that 'if it is not digital it did not happen,'" he stressed.

In his report, Mr. Heyns also cautioned that not all communities, and not all parts of the world, are equally connected, and draws special attention to the fact that "the ones that not connected are often in special need of protection."

"There is still a long way to go for all of us to understand fully how we can use these evolving and exciting but in some ways also scary new tools to their best effect," the expert stated, noting that not all parts of the international human rights community are fully aware of the power and pitfalls of digital fact-finding.

The Special Rapporteur made several recommendations in his report, including that the Office of the United Nations High Commissioner for Human Rights appoints as soon as possible a specialist in digital evidence to assist it in making the best use of ICTs.

B. Use of ICTs for Protecting the Right to Life

In 2015, Special Rapporteur Heyns produced a thematic report on the use of ICTs in protecting the right to life. The sub-headings of that report have been reproduced below, along with select examples from the Special Rapporteurs' other thematic reports, communications and country reports.

1. Promotion and advocacy

Report to the Human Rights Council (A/HRC/29/37, 24 April 2015, ¶¶44-48)

44. Greater capabilities for information sharing and communication present obvious and now widely used opportunities to disseminate information about human rights, either generally, as education, or as more focused advocacy in support of legislative or policy changes, or calling for investigation or accountability concerning individual cases. Human rights organizations can

supplement traditional communication strategies using mainstream media, by targeting the public directly.

45. Websites, for example, are used by intergovernmental and non-governmental organizations, as well as States, to make information about human rights norms or legal standards available to the widest possible audience. In previous reports, the Special Rapporteur underlined the importance of clear and publicly available legal frameworks for preventing arbitrary killings through the use of force or the application of the death penalty (A/HRC/26/36 and A/67/275).[8] ICTs clearly enable States to be more transparent towards their populations and the international community.

46. In addition to providing information digitally, many human rights organizations have developed expertise in using social media quickly and directly to engage members of the public. ICTs may create new educational opportunities that foster environments supportive of human rights. In Kenya, the PeaceTXT initiative sent peace-promoting text messages to registered subscribers with the aim of de-escalating potential conflicts. Elsewhere, NGOs have used secret filming to expose extreme cases of bigotry and harassment in order to sensitise public.[9]

47. Digital ICTs can thus facilitate the widespread visibility of human rights, at least among those connected through social media. Applications such as AiCandle or Pocket Protest allow users to sign petitions, write e-mails or receive human rights information using their mobile or smartphones and are particularly useful for urgent mobilizations.[10] Messages can also be amplified using platforms such as Thunderclap. Ultimately, such strategies can succeed in getting a case or issue on the public agenda.[11]

48. Questions remain as to whether these affordances are markedly changing advocacy dynamics for the better. Campaigns compete for attention in an ever-proliferating information context and are accessible – at least in the first instance – only to the digitally literate.[12] Meanwhile, the brevity of the messages and real-time culture of Twitter may preclude or simplify coverage of complicated situations and the drivers of virality can sit uneasily with human rights evidence.[13] Social networks are effective at increasing participation, in part because they lessen the motivation that participation requires, which can lead to shallow or fickle forms of activism (so-called "clicktivism").[14] However, some have argued that such seemingly insignificant moves are significant in their accumulation, demonstrating a "supportive environment" and "drawing awareness".[15]

With these greater opportunities for promoting human rights also come greater risks. Special Rapporteur Heyns had previously discussed this as part of his 2012 report to the Council on the protection of journalists:

8 ***Editors' Note:*** One of the projects undertaken during the mandate was the curation of an online resource collating national legislation about the use of force. This database has undergone a number of subsequent iterations, but can now be found at www.policinglaw.info.

9 Cynthia Romero, "What next? The quest to protect journalists and human rights defenders in a digital world", conference report, Freedom House, Mexico City, (February 2014), available at: https://freedomhouse.org/sites/default/files/What%27s%20Next%20-%20The%20Quest%20to%20Protect%20 Journalists%20and%20Human%20Rights%20Defenders%20in%20a%20Digital%20World.pdf.

10 See Amnesty International UK, "What is pocket protest?" (June 2013), available at: www.amnesty.org.uk/whatpocket-protest.

11 See Jiva Manske "Case studies: concrete examples of compelling and strategic use of social media", New Tactics in Human Rights (9 May 2013), available at: https://www.newtactics.org/comment/6124.

12 Thrall, Stecula and Sweet, "May we have your attention please?" *supra* note 5.

13 Dustin N. Sharp, "Human rights fact-finding and the reproduction of hierarchies" (6 June 2014), Social Science Research Network, http://papers.ssrn.com/abstract=2341186.

14 Malcolm Gladwell, "Small change: why the revolution will not be tweeted", *The New Yorker* (4 October 2010), available at: www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell.

15 Stephanie Vie, "In defense of 'slacktivism': the Human Rights Campaign Facebook logo as digital activism", First Monday, vol. 19, No. 4 (April 2014), available at: http://firstmonday.org/ojs/index.php/fm/article/ view/4961.

Report to the Human Rights Council (A/HRC/20/22, 10 April 2012, ¶36)

36. One of the main changes in the way in which the news is disseminated around the world in recent years has been the emergence of online journalists, both professionals as well as people who are untrained, who use social media. With the spread and increased availability of technology, the pool of who we now consider journalists has expanded rapidly, and so has the number of people who are potential targets of those who want to control the flow of information. In parts of Mexico, for example, the conventional media have for all practical purposes been replaced by new media—and assassins have likewise moved their sights.

2. Prevention and protection

Report to the Human Rights Council (A/HRC/29/37, 24 April 2015, ¶¶49-66)

49. ICTs can contribute to the prevention of violations of the right to life, by State or non-State actors, in a variety of ways. First of all, alert applications can provide physical and digital protection to potentially vulnerable groups, including human rights defenders. While that enables networks to take advantage of digital connectivity, the very same connectivity is a risk for those vulnerable to digital snooping or other forms of surveillance. Secondly, there is need for education on digital security and safety. Surveillance can, however, also be a preventive mechanism, and tactics ranging from live-streaming demonstrations or police operations to using satellite imagery will be discussed below.

1. Alert applications

50. Various organizations are developing alert applications that activists, journalists and others can use to send a signal that they are in danger. For example, Amnesty International developed a "panic button" application – disguised as an ordinary utility – that allows users secretly to activate an alarm by sending a text message, and, optionally, geolocation data, that can be sent to pre-selected contacts by rapidly pressing the power button of the phone. When activists or journalists are attacked or detained, their phones are often taken for the lists of contacts they store. The hidden application will continue to broadcast alerts, which are not only calls for help but also warnings to the person's contacts that they should take security precautions themselves.[16] Other applications or devices have been developed with the same objective.[17]

51. Such applications respond to the challenges posed by a lack of information and time lags, which can restrict efforts to protect individuals at risk. Practitioners believe that there is an approximately 48-hour window after an individual is detained or threatened during which a large-scale response is most likely to have the greatest effect. There are numerous examples worldwide in which mass response to detention – coordinated using social media or otherwise – has persuaded authorities to recalculate the merits of keeping an individual in custody.

52. The new technologies thus fit into wider and long-standing strategies of communicating with a trusted network when at risk and mobilizing a wide community to respond vocally or visibly to an arbitrary act against an individual. It is important, however, to bear in mind the potential risks of such technology which could become the basis of identification and targeting.

16 See https://panicbutton.io/.

17 *BBC News*, "Smart bracelet protects aid workers" (5 April 2013), available at: www.bbc.com/news/technology-22038012.

2. Importance of digital security

53. While they provide additional capabilities for those working on human rights issues, ICTs can present a number of additional risks, and to mitigate those risks, persons potentially at risk of violations, including human rights defenders, should take the requirements of digital security seriously. Digital security can include software to scan computers for spyware, resources such as Security-in-a-Box, as well as digital security helplines or forums.[18]

54. Activists can communicate more securely using virtual private networks, encryption programmes or Tor, a browser designed to increase the anonymity of Internet users. Nonetheless, developers and trainers should caution users that full privacy and anonymity online is never guaranteed. The risk of digital insecurity should also be weighed by larger international human rights actors, both intergovernmental and non-governmental, with regard to their interactions with smaller organizations or individuals.

55. Evaluating the merits and demerits of secure digital encryption does not fall squarely within the mandate of the Special Rapporteur. However, it is certainly a complex issue, with the demands of human rights investigation pulling in both directions, that becomes an issue of concern to this mandate holder when digital insecurity leads directly to victimization, including the threats or actual commission of extrajudicial killings. The use of mainstream social media platforms to share human rights information can pose security risks both for "civilian witnesses" and their subjects.

3. Monitoring for protection

56. The proliferation of surveillance and recording afforded by ICTs not only greatly enhances the opportunities to hold individuals to account, as will be discussed below, but can also prevent the commission of violations. Awareness of surveillance can have a significant deterrent effect if coupled with credible accountability regimes, as demonstrated by the use of closed-circuit television surveillance to deter crime. Belief in this deterrent effect is so strong that some activists have been known to pretend to film events, even though their phone battery was dead, as a strategy against abduction or arrest.[19]

57. Perhaps the most directly applicable example of this, and one that addresses a core interest of the Special Rapporteur – the excessive use of force by law enforcement – is the use of body-worn cameras by police officers. A recent study of the use of such technology in California, United States, found that officers' use of force dropped by 59 per cent on the introduction of the cameras, and complaints concerning excessive force dropped by nearly 90 per cent.[20] Other trial projects, involving the use of smartphones as body-worn cameras that transmit video, audio and geolocation information, are being run in Brazil, Kenya and South Africa.[21]

58. Just as the preventive impact of closed-circuit television works best where there is cognition of its presence, some argue that body-worn cameras deter violations because of their institutionalised

18 Resources provided through such programmes as New Tactics in Human Rights (www.newtactics.org) provide spaces for online knowledge exchange on various aspects of human rights work, including digital security

19 Stephanie Hankey and Daniel Ó Clunaigh, "Rethinking risk and security of human rights defenders in the digital age", *Journal of Human Rights Practice*, 5 (November 2013), p. 543.

20 Barak. Ariel, William A. Farrar and Alex Sutherland, "The effect of police body-worn cameras on use of force and citizens' complaints against the police: a randomised controlled trial", *Journal of Quantitative Criminology* (November 2014).

21 Graham Denyer Willis and others, "Smarter policing: tracking the influence of new information technology in Rio de Janeiro", Igarapé Institute Strategic Note 10 (November 2013); see also the Smart Policing initiative, http://en.igarape.org.br/smart-policing/.

use, whereby the police must issue a warning that incidents are being recorded, which creates cognition of surveillance among both police and civilians.[22]

59. Concerns exist around possible violations of the right to privacy that body-worn cameras may generate, leading to suggestions that they be turned off upon entering a home or when speaking with victims. Others consider that individual officers should not have control over their cameras, so as to reduce opportunities for selective documentation.[23] Concerns also exist with respect to access to and secure storage of the footage. Although questions remain to be answered, many feel that the deterrent effect of police body-worn cameras warrants further deployment.[24] Linked with the potential advantages of the police recording themselves is the equally important protection of citizens' right to record the police.

60. If body-worn cameras bring surveillance to the micro level of interpersonal interactions, at the opposite end of the spectrum is the surveillance potential of remote sensing imagery, either from satellites or drones. Initiatives such as the Satellite Sentinels Project and Amnesty International's Eyes on Darfur campaign have highlighted the possibilities of such mechanisms. Raising awareness among potential perpetrators that vulnerable areas are being watched could deter violations, or at least those that are visible remotely.[25] However, such surveillance is expensive and can involve rather arbitrary decisions about which communities or places to monitor. As with other surveillance methods, the deterrent effect of the technology is connected to both awareness of its existence (making the accompanying media campaign significant) and the credible threat of punitive measures.[26]

61. Those surveillance methods use the threat of accountability in the future to condition behaviour in the present. It is potentially also possible to exploit the capacities of ICTs to use information from the (recent) past to influence what happens in the present. Social media analysis could predict hotspots of human rights violations in real time. For example, the Hatebase database collects data on the vocabulary and incidence of hate speech on social media based on the correlation between hate speech and the risk of genocide and is used to predict regional violence. [27]

62. There are limitations, however, to the possibilities of ICTs as early warning systems. Although "big data mining", i.e. collecting large amounts of data, has a record of being good for conflict prediction and prevention, it has been less effective for analysis and actionable transmission.[28]

63. Big data mining and remote sensing work for the prevention of human rights violations also raises methodological and ethical concerns. For example, vulnerable populations could be put at risk by the remote documentation, and thus identification, of their locations and situations.[29]

22 The effect of cognition of surveillance was perhaps most memorably elaborated by Jeremy Bentham, but its criminological effects, as well as its potential dangers, have not been technologically realised until recently.

23 Bracken Stockley "Public support for police body cameras – but who controls on/off switch?" The justice gap (March 2014), available at: http://thejusticegap.com/2014/03/body-worn-video-cameras-scrutiny/.

24 Robert Muggah, "Why police body cameras are taking off, even after Eric Garner's death", IPI Global Observatory (11 December 2014), available at: http://theglobalobservatory.org/2014/12/ police-body-cameras-eric-garner/; see also Alexandra Mateescu, Alex Rosenblat and Danah Boyd, "Police body-worn cameras", Data & Society Research Institute Working Paper (February 2015), available at: www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf.

25 Nathaniel A. Raymond et al. "While we watched: assessing the impact of the satellite sentinel project", Georgetown Journal of International Affairs (26 July 2013), available at: http://journal.georgetown.edu/ while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-etal/.

26 Ibid.

27 See http://www.hatebase.org/.

28 Sheldon Himelfarb, "Can big data stop wars before they happen?" (United States Institute of Peace, 25 April 2014), available at: www.usip.org/publications/can-big-data-stop-wars-they-happen.

29 See, for example, Harvard Humanitarian Initiative, "The Signal Program on Human Security and Technology"

Moreover, potential inaccuracies in the statistical analysis of human rights data arise from selection bias, duplication and constraints on data capture.[30]

4. Towards digital due diligence

64. The application of surveillance to prevent violations of human rights may be so effective as to imply that States with the capacity to take advantage of them have a responsibility to do so. Cameras have been used in police vehicles and interrogation rooms and consideration might be given to other contexts in which such surveillance could have a preventive effect (for example, prisons), subject to the limitations imposed by other rights, such as the right to privacy.

65. Other affordances of ICTs can be harnessed by States to fulfil their responsibilities concerning prevention or precaution. For example, there have been instances of States using text messages or calls to warn civilian populations before launching air raids. The recording devices on certain advanced weaponry offer the potential for greater oversight, but that will require more transparency.

66. In the digital space, however, the responsibility of due diligence extends beyond States. Human rights monitoring organizations – both intergovernmental and nongovernmental – need to give thought to the consequences of their correspondence or use of information. Traditional understandings of "informed consent" may need to be revisited.

In a number of their investigations, the Special Rapporteurs encountered (and suggested) ways in which ICTs can be harnessed to protect the right to life. In 2005, in response to the extrajudicial execution of a human rights defender, the government of Brazil described its efforts to compile a central database of threats and actions against human rights defenders.

Allegation letter sent to the Government of Brazil (4 March 2005) (with the Special Representative of the Secretary General on the situation of human rights defenders and the Special Rapporteur on the independence of judges and lawyers)

Sister Dorothy Stang, an environmentalist, human rights defender and member of the Pastoral Land Comission (*Comissão Pastoral da Terra*), an organization of the Catholic Church which works to promote and defend the rights of rural workers and land reforms in Brazil was shot on 12th February 2005 at approximately 9.00am. She was shot several times, resulting in her death, as she walked to attend a meeting in the town of Anapu, Pará.

Response of the Government of Brazil (17 May 2005)

In an additional response dated 17 May 2005, the Government of Brazil informed the Special Rapporteurs that by decree No 66 and 89/2003 it has established a working group to elaborate a National Programme for the Protection of Human rights Defenders that was launched on 26 October 2004 at the Parliamentary Commission on Human Rights. Members of the Government and the civil society have participated to this new initiative. The National Congress has approved a budget of one million two hundred thousand *reais* to finance this programme. The Congress is also currently working on a draft law N03616/2004 including a chapter for the protection of victims and witnesses of human rights violations under threat. Within this Protection Programme, a database compiling all human rights violations as well as threats against human rights defenders is being set up in nine pilot-States, namely Paraíba, Pará, Rio Grande do Norte, Pernambuco, Bahía, Espírito Santo, Sâo Paolo, Mato Grosso et Paraná. Further efforts are being made in Espiríto Santo, Pará and Pernambuco to establish a methodology and standards of emergency procedures for the

(2013), see: http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-earlywarning/signal-program.

30 See the work of the Human Rights Data Analysis Group, https://hrdag.org/coreconcepts/.

protection of Human Rights Defenders. The Protection Programme in the Pará State was established in February 2005. The killing of Sister Stang has triggered the implementation of an emergency programme. Lists of human rights defenders under threat were constituted, investigations of suspected military and civilian police officers were carried out. Similar programmes are being established in the States of Espirito Santo, Pará, and Pernambuco.

In Colombia, Special Rapporteur Alston highlighted the potential benefits of a central database of investigations into extrajudicial executions, but cautioned authorities to be mindful of privacy concerns.

Report on Mission to Colombia (A/HRC/14/24/Add.2, 31 March 2010, ¶¶85-86)

Victims' access to information

85. Coordinating and tracking the results of investigations by the various institutions is problematic and victims' family members justifiably complained about the difficulty of obtaining information about the status of cases. A relatively easy and inexpensive solution would be a centralised database system through which each institution reports its activity and progress on each individual case. Information from this system should be available through institutional representatives at the regional, municipal and community level, so that families would not need to travel long distances to obtain it. Responsibility for maintaining the system and ensuring that all institutions comply with reporting obligations could be assigned to the Office of the Vice-President or another Government unit; the key is that it be an institutional actor with the stature to enforce reporting obligations.

86. Given the influence of IAGs [illegal armed groups] or guerrillas on officials in some local communities, the database should not include sensitive information that could expose witnesses and victims' families to greater security risks. Nor should it include genuinely confidential information related to ongoing investigations or prosecutions (family members could be directed to the local *fiscal* for that information).

In discussing the government of Ecuador's response to the problem of homicide and hired killings, Special Rapporteur Alston described its use of geolocating and policing the online sphere.

Report on Mission to Ecuador (A/HRC/17/28/Add.2, 9 May 2011, ¶¶25-27)

25. The Government now acknowledges the seriousness of the problem, and in 2010 began to take strong measures to address it.

26. Expert advisers have been brought in from Colombia and France to assist at the policy level, and an inter-agency police team has been created to coordinate the police response. Importantly, a specialised police intelligence group (*Unidad de la Lucha Contra el Crimen Organizado* or ULCO) has been created to counter organised crime, including by researching the methods employed by hired killers and the causes of the killings. Witness protection is being strengthened, and rewards will be offered for information on organised crime activity.

27. In some cities, stronger steps have been taken to "geo-reference" criminal incidents, so that police patrols can be increased in especially affected areas, and greater attention has been given to the loan shark problem. The police also indicated that more would be done to investigate online advertisements posted by would-be hit men. In Guayas, motorcycles were required to display registration details, which led to a small drop in killings. Controls were also placed on alcohol consumption, and efforts were increased to close non-licensed premises.

In 2014, Special Rapporteur Heyns urged the government of Mexico to use ICTs in regulating the use of force by its agents.

Report on Mission to Mexico (A/HRC/26/36/Add.1, 28 April 2014, ¶¶48-49)

48. The Special Rapporteur recalls that in both investigations and prosecutions, the powers of modern technology can enhance the efforts of the State to ensure greater accountability, thus reducing its reliance on the use of force. He recommends that Mexico make greater use of the superior access it has to intelligence networks and regional cooperation to counter organised crime and abuses by security forces which threaten the right to life.

49. He underlines that this should have two interlinked components. On the national level, databases should be created *inter alia* in the areas of fingerprinting, DNA, genetics, unidentified remains, and missing persons and should be made digital and linked. Moreover, Mexico should play an increasingly active role in linking up with other States, especially in Central America, to ensure that such information is also shared with the security services of those States.

ICTs have afforded almost anyone with a camera or cellphone the ability quickly and easily to record events. In 2016, in his joint report to the Council on the proper management of assemblies, Special Rapporteur Heyns discussed the right to observe, monitor, and record such events.

Joint Report (with the Special Rapporteur on the rights to freedom of peaceful assembly and of association) on the proper management of assemblies (A/HRC/31/66, 4 February 2016, ¶¶68-71)

F. Every person shall enjoy the right to observe, monitor, and record assemblies

68. All persons enjoy the right to observe, and by extension monitor, assemblies. This right is derived from the right to seek and receive information, which is protected under article 19 (2) of the International Covenant on Civil and Political Rights. The concept of monitoring encapsulates not only the act of observing an assembly, but also the active collection, verification and immediate use of information to address human rights problems.[31]

69. A monitor is generally defined as any non-participant third-party individual or group whose primary aim is to observe and record the actions and activities taking place at public assemblies.[32] National human rights institutions, ombudsmen, intergovernmental entities and civil society organizations all commonly act as monitors. Journalists, including citizen journalists, play an important role.[33]

70. States have an obligation to protect the rights of assembly monitors. This includes respecting and facilitating the right to observe and monitor all aspects of an assembly, subject to the narrow permissible restrictions outlined in article 19 (3) of the International Covenant on Civil and Political Rights. Monitors retain all other human rights. The State should fully investigate any human rights violation or abuse against monitors, and should pursue prosecution and provide adequate remedy. The protections afforded to monitors apply irrespective of whether an assembly is peaceful.

71. Everyone – whether a participant, monitor or observer – shall enjoy the right to record an assembly, which includes the right to record the law enforcement operation. This also includes the right to record an interaction in which he or she is being recorded by a State agent – sometimes referred to as the right to "record back". The State should protect this right. Confiscation, seizure

31 Office of the United Nations High Commissioner for Human Rights, *Training Manual on Human Rights Monitoring* (United Nations publication, Sales No. E.01.XIV.2), para. 28.

32 Office for Democratic Institutions and Human Rights (ODIHR) of the Organization for Security and Cooperation in Europe (OSCE), *Guidelines on Freedom of Peaceful Assembly* (2010), para. 201.

33 See, for example, OSCE, "Special report: handling of the media during political demonstrations" (2007).

and/or destruction of notes and visual or audio recording equipment without due process should be prohibited and punished.

3. Monitoring and fact-finding

Country missions by the Special Rapporteurs, as well as by NGOs, commissions, and other investigatory bodies, are heavily dependent upon fact-finding. In his final report to the General Assembly, Special Rapporteur Alston reviewed new technologies in fact-finding, and called upon human rights factfinders to be more proactive in their use of new technologies, and for the Office of the High Commissioner to convene an expert group to examine the issues.

Report to the General Assembly (A/65/321, 23 August 2010, ¶¶6-10, 46-47)

6. New social media, social networking sites, user-generated content sites or platforms, and a range of other information and communications technologies enable any person with access to the necessary technology to share and report information relating to killings or other human rights violations in real time, for example, through Facebook, Twitter, or crowdsourcing technologies[34] such as Ushahidi. The Ushahidi platform, for example, originally developed largely by Kenyans during their country's 2007-2008 post-election violence, allows users to submit reports of human rights abuses by text message (SMS), smart phone application, Twitter, e-mail or the Web. Information, such as the time, location, nature of a human rights abuse, and pictures and video footage, can then be geo-tagged and plotted on a map or timeline. The platform has since been used in a range of situations, including in the Democratic Republic of the Congo, South Africa, Gaza, India, the Sudan, Afghanistan, Burundi, and following the January 2010 Haiti earthquake. The possibilities for increasing the speed, depth, and scope of human rights monitoring with crowdsourcing and SMS reporting platforms (such as Frontline SMS) are readily apparent. With hundreds or thousands of users, the platform can be used as an early warning system, or to track patterns of violence or the effects of a natural disaster, or to facilitate rapid response or service delivery. Crisis mapping[35] can provide important visual representation of events, facilitating more effective strategic planning or advocacy. Cell-phone based reporting systems have also been harnessed to improve the provision of health and humanitarian assistance, and environmental conservation.[36] The technologies may also allow users to get around biases in mainstream media or Government censorship, as the use of Twitter in the Islamic Republic of Iran famously demonstrated, enable reporting from areas where fact-finders cannot themselves physically access, and generally increase public participation in human rights advocacy.[37] A range of wikis and user generated content or collaborative websites,

34 In general terms, crowdsourcing is an open invitation to a population to provide information and ideas. More specifically, the term is often used to refer to crowdsourcing via web 2.0 technologies. See generally: Ankit Sharma, "Crowdsourcing Critical Success Factor Model" Working Paper (2010), and sources cited therein; Karthika Muthukumaraswamy, "When the Media Meet Crowds of Wisdom", *Journalism Practice* 4 (24 July 2009); Jeff Howe, "The Rise of Crowdsourcing", available at: www.wired.com (2006); and Anand Giridharadas, "Africa's Gift to Silicon Valley: How to Track a Crisis", *The New York Times* (12 March 2010).

35 See http://www.crisismappers.net/; http://irevolution.wordpress.com/2009/08/08/proposingcrisis-mapping/; http://hhi.harvard.edu/programs-and-research/crisis-mapping-and-earlywarning. See also the United Nations Development Programme's Threat and Risk Mapping Analysis in the Sudan, at http://www.sd.undp.org/projects/dg13.htm.

36 For example, the United Nations Children's Fund (UNICEF) has used cell-phone reporting systems in the provision of humanitarian aid. In Ethiopia, UNICEF used RapidSMS to better distribute food supplies. See "Preventing Famine with a Mobile" (21 December 2008) at www.mobileactive.org. See also See Sheila Kinkade and Katrin Verclas, "Wireless Technology for Social Change: Trends in Mobile Use by NGOs", United Nations Foundation-Vodafone Group Foundation Partnership (2008).

37 See Molly Beutz Land, "Networked Activism", *Harvard Human Rights Journal* 22 (2009); Geoffrey A. Fowler, "'Citizen Journalists' Evade Blackout on Myanmar News", *The Wall Street Journal* (28 September 2007).

such as Wikileaks, OpenStreetMap (an editable street map of the world), YouTube,[38] and the Hub[39] can serve similar functions.

7. But there are also significant obstacles to effective human rights applications of these technologies. Credibility and reliability of information are primary concerns in fact-finding. The reporting and advocacy that follow human rights investigations are open to challenge and can readily be impugned where the "facts" themselves were gathered through unreliable methodologies, or by inexperienced, or biased fact-finders. Crowdsourcing, for example, potentially creates "a tsunami of unverified reporting".[40] Because of the very real concern that crowdsourced information could contain erroneous or falsified data,[41] at this stage, it would be difficult to conceive of a human rights report based solely on crowdsourced information. But crowdsourcing could certainly be used by organizations (e.g. national human rights institutions, ombudsmen, non-governmental organizations) to receive notifications of alleged abuses which could then be tracked and investigated, or crowdsourced platforms could be bounded so that only certain trusted sources (e.g. United Nations or other designated local field investigators) could provide information to it.[42] Some programmes are also being developed to address reliability and accuracy concerns – SwiftRiver, for example, uses natural language computation, machine learning, and veracity algorithms to aggregate, filter, and triangulate information from online news, blogs, Twitter, SMS, and other sources.[43]

8. Crowdsourcing can also raise privacy and security concerns for those reporting abuses. Such concerns demand careful consideration before the technology is deployed in sensitive environments. For example, a repressive Government might monitor text messages sent to a platform, or require the registration of personal information by those involved.[44] Other problems can arise with coordination and information-sharing. Thus in the aftermath of the Haiti earthquake it was observed that each system was an island of information, leading to unnecessary duplication, fragmentation and significant frustration.[45] Other important concerns include uneven access to technologies (which may result in distorted findings or advocacy focus), sustainability (especially after the urgency of a particular crisis appears to fade), the expense and reliability of cell networks or Internet connections, and potential users' training and knowledge. The humanitarian, disaster

38 See Larry Diamond, "Liberation Technology", *Journal of Democracy* 21 (2010) 76 (referring to a range of "liberation" and "accountability" technologies, and giving YouTube as an example of a tool "for transparency and monitoring": "Enter 'human rights abuses' into YouTube's search box and you will get roughly ten thousand videos showing everything from cotton-growers' working conditions in Uzbekistan, to mining practices in the Philippines, to human-organ harvesting in China …").

39 The Hub is a project of the international organization WITNESS. WITNESS provides training and equipment on using video technologies to record human rights abuses. The Hub is a website where human rights videos can be shared.

40 See United States Department of State, "Haiti Earthquake: Breaking New Ground in the Humanitarian Information Landscape" (July 2010), p. 4.

41 See Anahi Ayala Iacucci, "Ushahidi-Chile: an example of crowdsourcing verification of information" available at: http://crisismapper.wordpress.com/2010/06/28/ushahidi-chile-an-example-ofcrowd-sourcing-verification-of-information/ (discussing false reports made following the Chile Earthquake); Peter Smith, "Cellphone and Internet access helps – and hinders – accurate reporting in Kenya", at www.csmonitor.com (31 January 2008) (discussing false information and rumours).

42 See, for example, Peter van der Windt, "Voix des Kivus (Ushahidi in the Democratic Republic of the Congo)", talk given at the International Conference on Crisis Mapping (2009) (discussing a pilot project on the eastern Democratic Republic of the Congo, providing cell phones to village leaders to report abuses via SMS).

43 See http://swift.ushahidi.com.

44 See Patrick Meier, "How to Communicate Securely in Repressive Environments" (15 July 2009) at http://irevolution.wordpress.com/2009/06/15/digital-security/.

45 ICT for Peace Foundation, "Haiti and beyond: Getting it right in Crisis Information Management" (March 2010).

relief, and ICT communities are presently engaged in an important discussion of these problems,[46] much of which is relevant to human rights actors.

9. Geospatial technologies also have enormous potential to aid in human rights work, and some organizations are beginning to use them in their investigations and advocacy.[47] Amnesty International, for example, as part of its "Science for Human Rights" programme (together with the American Association for the Advancement of Science[48]), is using mapping and satellite imagery to provide supporting evidence to witness accounts and to document abuses (such as the destruction of homes or villages), and to provide interactive visual information in its advocacy work.[49] Satellite imagery, however, can be very expensive to purchase, may need to be obtained from Governments, and can be limited by factors such as time lag and cloud interference. In response, some have suggested or begun to develop unmanned aerial vehicles or other aerial photography mechanisms for humanitarian purposes (which could similarly be used in the human rights field), although the actual use of these are currently inhibited by problems of insurance and regulation issues for the civilian use of unmanned aerial vehicle.[50]

10. Other technologies, including artificial intelligence,[51] robotics,[52] Photosynth,[53] and hyperspectral imagery[54] also have potential but largely unexplored human rights applications.

46 See the work of Patrick Meier at http://irevolution.wordpress.com/; compare http://www.humanitarian.info/2009/03/30/correcting-crowdsourcing-in-a-crisis/. See also "Breaking New Ground in the Humanitarian Information Landscape", footnote 9 above.

47 See International Crisis Group, "War Crimes in Sri Lanka" (17 May 2010) (referring to satellite imagery providing evidence of abuses); Human Rights Watch, "Georgia/Russia: Use of Cluster Munitions in August 2008" (9 April 2009) (providing maps and satellite images of the location of cluster munitions use); Human Rights Watch, "Israel/Gaza: Satellite Imagery of White Phosphorous Use" (25 March 2009). See also, the World Food Programme's use of satellite imagery: http://www.wfp.org/our-work/our-competences/being-ready/technology-helping-wfp. See also: David Talbot, "Satellite Images Catch Human-Rights Violations in Burma", *Technology Review* (28 September 2007). For uses of Google Earth, see: MapAction, "Google Earth and its potential in the humanitarian sector: a briefing paper" (April 2008).

48 The AAAS has a dedicated "Science and Human Rights Program", including a "Geospatial Technologies and Human Rights Project". See AAAS, "What can geospatial technologies do for the human rights community?" available at: http://shr.aaas.org/geotech/whatcanGISdo.shtml. See also Tactical Technology Collective, "Maps for advocacy: An introduction to Geographical Mapping Techniques" (September 2008).

49 For example, Amnesty International's "Eyes on Darfur" project brings together satellite imagery, witness accounts, and ground photos to evidence and illustrate abuses in Darfur. The satellite images show villages before and after destruction. See http://www.eyesondarfur.org/about.html. The "Eyes on Pakistan" project uses interactive maps to show the locations of attacks on civilians: http://www.eyesonpakistan.org/.

50 See H. Bendea et al, "Low Cost UAV for Post-Disaster Assessment", *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Science*, Vol. XXXVII (2008) (describing the development of low cost UAVs for early impact analysis of humanitarian disasters, and their advantages); Bendea et al, "New Technologies for Mobile Mapping", paper presented at the fifth International Symposium on Mobile Mapping Technology (2007).

51 See, for example, Artificial Intelligence for Development, at http://ai-d.org/index.html.

52 See e.g. John G. Blitch, "Artificial Intelligence Technologies for Robot Assisted Urban Search and Rescue", *Expert Systems With Applications* 11 (1996) (discussing the use of mobile robots to rescue individuals trapped in collapsed structures). See also: IRIN, "Bots without borders" (22 June 2009) available at: http://www.irinnews.org/Report.aspx?ReportId=84933 (discussing the potential for automated humanitarian relief); http://www.humanitarianfutures.org/main/content/science-panel; http://crasar.org/.

53 Photosynth allows users to create a three-dimensional model of a series of photographs uploaded to the site. If, for example, a number of users took photos at the scene of an alleged human rights violation, the photos could all be "stitched" together to create a compilation of many images taken from different perspectives; this could be an important evidence gathering tool. See http://photosynth.net/about.aspx; Sanjana Hattotuwa, "Information visualization through Microsoft Photosyth: Potential for human rights documentation?" (31 July 2008) at http://ict4peace.wordpress.com.

54 See Margaret E. Kalacska et al, "The Application of Remote Sensing for Detecting Mass Graves: An Experimental Animal Case Study from Costa Rica", *Journal of Forensic Sciences* 54 (2008).

[...]

46. Human rights methodologies have tended to be dominated by a catch-up mentality. The assumption often seems to be that new approaches should be considered only after it has become patently obvious that existing approaches are no longer adequate. This needs to change and the United Nations, as well as Governments and civil society groups, should adopt a much more proactive approach. …

47. The Office of the United Nations High Commissioner for Human Rights should convene an expert group of information and communication technology experts, humanitarian and human rights actors with experience using new technologies, and relevant private sector representatives to discuss the current and potential human rights applications of new technologies and the obstacles to their effective use. The group should also address: how to protect the security of those reporting abuses (e.g. location tracking; protected data transmission technologies); how to improve access to and use of satellite and other aerial imagery; the use by human rights actors of crowdsourcing platforms to receive allegations of abuses; how to promote the use of new technologies and outreach to local communities; how to measure the impact of ICT on the promotion of human rights; and what type of new international standards, if any, should be developed in this area.

In his 2015 report to the Council, Special Rapporteur Heyns reaffirmed many of the same points about the potential power of civilian documentation for human rights accountability, along with the possible other affordances of technology to collect information about human rights violations.

Report to the Human Rights Council (A/HRC/29/37, 24 April 2015, ¶¶67-76)

67. As noted above, the particular nature of violations of relevance to this mandate place a premium on fact-finding. Human rights organizations have developed rigorous fact finding methodologies, not least to protect the credibility of their evidence, and thus their reputations. ICTs and the user-generated content they facilitate have broadened and democratised the process of fact-finding by empowering both spontaneous and solicited "civilian witnesses." The most challenging dimension of this evolution is balancing democratization with a continued, perhaps heightened, requirement for authority and thus for verification of digital evidence.

1. Civilian witnesses and video evidence

68. The advantages of video evidence have been appreciated by campaigners for several decades, at least since the Rodney King incident in the early 1990s. The re-purposing of private closed-circuit television footage for public investigations has become commonplace.[55] At the international level, the conviction by the International Criminal Court of Thomas Lubanga, which admitted video footage of interviews of child soldiers who had been impressed into his militia, proved that video recordings could be used to fill an evidentiary gap.[56] Of course, it is not only witnesses or subjects of violations who are producing such information, but also perpetrators. Moreover, information does not have to be shared publicly for it to be useful to human rights investigations.

69. While information from civilian witnesses has long been a cornerstone of human rights fact-finding, it has traditionally been gathered by professionals. Either professionals or their trusted contacts would be present during the production and transmission of information from witness

55 See, for example, Daoud Kuttab, "Video technology exposing Isreali violations in the West Bank", *Al-Monitor* (8 July 2014), available at: www.al-monitor.com/pulse/originals/2014/07/israel-palestine-cctv-camerafootage-occupation-settlers.html.

56 Matthew Shaer, "The media doesn't care what happens here: can amateur journalism bring justice to Rio's favelas?" *The New York Times* (18 February 2015), available at: www.nytimes.com/2015/02/22/ magazine/the-media-doesnt-care-what-happens-here.html.

to fact-finder during an interview, for example. ICTs enable civilian witnesses autonomously to produce and transmit information.

70. At its most spontaneous, civilian witnessing can occur through widely available consumer tools or platforms. The ubiquity of smartphones enables the capture of visual and auditory information, which can be easily transmitted through digital channels such as social media platforms. The benefit of those production and transmission strategies is that they do not require any particular expertise; the drawback is that they may limit the metadata (such as source, place and time of production) which could be instrumental to verifying the information. Alternatively, applications such as InformaCam and EyeWitness are specifically designed to enhance the metadata supplied with photographic or video information and to maintain the chain of custody.[57]

71. A number of NGOs are already offering training courses to citizen witnesses and trainers on how to produce and transmit material with stronger evidentiary value. WITNESS, Amnesty International, Tactical Tech and the Open Society Justice Initiative are all conducting such activities on a global or regional scale. The training may concern both personal protection issues, such as those concerning digital security, discussed above, and practical information about the kind of detail to capture in witness videos (such as licence plates, uniform numbers or landmarks) and how to share them.[58]

2. Crowdsourcing information

72. Somewhere between the traditional methods of soliciting information from civilian witnesses and the spontaneous production and transmission of information by civilian witnesses are the practices of crowdsourcing and crowdseeding. Crowdsourcing involves turning over tasks to a large, unspecified group recruited through an open call but that is not necessarily representative, as such calls privilege the participation of those with resources such as technology, money and time. Crowdseeding is a form of bounded crowdsourcing whereby participants can be randomly sampled for representativeness and equipped with the technology and resources necessary for gathering information. A relationship develops over time between chosen witnesses and the project, with the credibility and trust that such a relationship entails.[59]

73. Besides potentially widening the scope of human rights work, involving civilian witnesses as a crowd could strengthen the effect of human rights advocacy through greater participation and awareness as well as potential corroboration.[60] However, there are risks. By publicly mapping information, crowds may jeopardise vulnerable populations. The techniques may also be used against the human rights community, for example to perform "human intelligence tasks" such as matching faces to photographs of protests.[61]

3. Satellite evidence

74. Satellite footage can have a transformative impact on human rights work. Central to the deterrent effect of satellites is the knowledge that, should a violation occur, somebody is going to use the footage to expose it. For example, earlier this year, fact-finders at Amnesty International

57 See information about Informacam, https://guardianproject.info/informa/; and New Perimeter, "eyeWitness to atrocities", www.newperimeter.org/our-work/access-to-justice/eyeWitness.html.

58 See, for example, Kelly Matheson, "Video as evidence: basic practices", *Witness blog* (16 February 2015), available at: http://blog.witness.org/2015/02/video-as-evidence-basic-practices/.

59 Patrick Meier, "From crowdsourcing crisis information to crowdseeding conflict zones (updated)", *iRevolutions* (10 July 2012), http://irevolution.net/2012/07/10/crowdsourcing-to-crowdseeding/.

60 Molly Beutz Land, "Peer producing human rights", *Alberta Law Review*, 46:4 (2009), p. 1115.

61 Jonathan Zittrain, "The Internet creates a new kind of sweatshop", *Newsweek* (7 December 2009), available at: www.newsweek.com/internet-creates-new-kind-sweatshop-75751.

and Human Rights Watch undertook "change detection" analysis of satellite images of two towns in north-eastern Nigeria that revealed extensive fire damage. The information was cross-referenced with eyewitness testimonies to establish that the fires were part of militant attacks in which hundreds were killed. Although that linking was important because, on their own, satellite images do little to establish culpability and causality, the case highlights the benefits of remote sensing for hard-to-reach areas.[62]

75. Satellite evidence can be combined with other digital processes, such as social media mapping, in order to better convey information. Reports on the origins of missile or artillery attacks or the impacts of drone strikes have relied on satellite photography.[63]

76. At present, much of the satellite imagery relied on for human rights work is owned by commercial operators. This means that, for satellite imagery to be available, there must be a commercial interest in the area and no cloud cover; also, the imagery will tend to be of low resolution. Military-grade satellite imagery has broader coverage and higher resolution, but there is often a reluctance to share information (rather than classified imagery itself) with human rights investigators, even when national security is not at stake

4. Evaluating evidence collected using ICTs

One of the particular challenges associated with ICTs in the human rights sphere is how best to harness their evidentiary potential. Special Rapporteur Heyns addressed this issue in his 2015 thematic report to the Human Rights Council.

Report to the Human Rights Council (A/HRC/29/37, 24 April 2015, ¶¶77-91, 100-106)

E. Evaluating evidence collected using information and communications technologies

77. The flood of information from civilian witnesses can only have evidentiary potential if the information can be gathered and evaluated. It is therefore important that human rights organizations be able to integrate that information into their traditional methods of research and analysis, especially given the importance of reporting credibility. However, evaluating digital content produced by civilian witnesses can be a challenge, including with regard to the identification of relevant information, and verification and storage of that information. Technological developments as well as initiatives in information evaluation practices may help to address those challenges.

1. Problem of volume

78. The proliferation of digitally produced and transmitted civilian witness information means that identifying relevant information can be an overwhelming task. Using networks to crowdsource the filtering process can be an intermediary step, but it will likely be necessary to harness the analytical affordances of digital ICTs to address their own "signalto-noise ratio" problem. One way is through the automated cleansing of large datasets of potentially relevant information. For example, CrisisNET aims to collect and standardise real-time digital crisis data from thousands of sources so that researchers can search quickly and efficiently.[64] Although machines cannot replace human expertise in the evaluation of human rights information – for assessing the relevance of

62 Christoph Koettl, "The story behind the Boko Haram satellite images", Amnesty International UK/Blogs (17 January 2015), available at: www.amnesty.org.uk/blogs/ether/story-behind-boko-haram-satelliteimages.

63 Bellingcat, "Origin of artillery attacks on Ukrainian military positions in Eastern Ukraine between 14 July 2014 and 8 August 2014" (17 February 2015), www.bellingcat.com/news/uk-andeurope/2015/02/17/origin-of-artillery-attacks/; and Forensic Architecture, "Drone strikes: investigating covert operations through spatial media", www.forensic-architecture.org/case/dronestrikes/.

64 See http://crisis.net/about/.

information for evidence is an ultimately subjective task —, technology can help human rights monitors to concentrate on the most important material. More research is needed in this regard.

79. There will probably always be a need to curate digital content for monitoring and consumption by a wide audience of interested parties. Such curation will involve a combination of automation and traditional fact-finding or verification skills. One successful model is the WITNESS Human Rights Channel, which uses material that is verified in partnership with the social media news agency Storyful.

2. Problem of transience

80. Because much of the material of relevance to human rights investigations could be online for only a very limited time (owing to pressures either on the uploader or the platform not to host content of a certain type),[65] it is important that investigators have the capacity to capture all the information that might be needed and to store it securely. The development of guidelines for national investigators as well as human rights monitors should be a priority.[66]

81. The storage of material for human rights investigations can be a security risk for activists. Applications such as Eyewitness and International Evidence Locker have been designed to allow witnesses to upload evidence to a cloud-based repository and to use or delete it as best suits their circumstances. Those applications also allow secure transmission of information to target audiences while maintaining the metadata of the information as well as the information itself. Nonetheless, collaboration between investigators and technology corporations will remain a vital consideration.

3. Problem of verification

82. Although sometimes raised as a major impediment to the embrace of digital evidence, verification is not a new issue: it concerns the conventional institutional need to establish the credibility of a source and the accuracy of its information before acting on or staking one's reputation to a claim. While the nature of the information being verified and the specific techniques are shifting rapidly as ICTs evolve, the fundamentals of verification remain constant: identifying and corroborating the content and provenance of information received.

83. Verification usually involves checking the origin, source, time and place of the information in question, as well as the chain of custody. Fact-finders must take time to establish the identity of the source, assess the file for metadata indicators, then cross-reference those with other sources. A new set of methods, often referred to as information forensics, is emerging, but many elements of the process still require human expertise and painstaking checks, akin to old-fashioned investigation.

84. The witness may provide information concerning the time, place and content in an interview, or, alternatively, may include that information in the file. The former method underlines the importance of cross-fertilization between the methodology of the second and third generations of fact-finding and the extent to which the sources of one can bolster the authority of the other, while the latter can occur either during the production process, for example by verbalizing the location and date, or through the transmission process. The information may also be evident through physical landmarks (such as road signs or geological features), weather conditions, clothing, weapons or dialect captured in the digital file, or it may also be identified through the metadata

65 Madeleine Bair, "Navigating the ethics of citizen video: the case of a sexual assault in Egypt", *Arab Media & Society*, 19, (2014), available at: http://arabmediasociety.com/?article=844.

66 Resources exist to guide activists concerning the archiving of their material, for example, see http://archiveguide.witness.org/. The Office of the Prosecutor of the International Criminal Court is currently finalizing guidelines for investigators.

automatically embedded in the file, such as the time stamp. That information can be corroborated and cross-referenced against other digital files and evidence, including satellite images. Several videos of the same incident can be time synced so as to provide a multi-perspective video timeline.[67]

85. Recognition of the need for expertise concerning digital verification is growing. The more knowledge about information forensics that human rights fact-finders have, the more comfortably and quickly they will be able to use digital information from civilian witnesses. The Verification Handbook, published in 2014, quickly became a reference point for humanitarians and human rights fact-finders.[68]

86. Increasing verification knowledge among civilian witnesses is likely to ease the verification process. WITNESS, for example, provides a guide on what information to include in videos documenting human rights violations.[69]

87. Another strategy to facilitate verification is through initiatives that support either the provision of information for verification or the evaluation of that information. Such initiatives have been referred to as "verification subsidies" and may incorporate human participation or designed technologies.[70] Applications such as InformaCam automate the addition of verification cues at production and prompt their inclusion during transmission. Alternatively, the power of the crowd can be used retrospectively, as is done, for example, with Veri.ly.[71] Alternatively, Checkdesk, a platform designed for individual newsrooms, allows for collaborative and transparent verification among members of a bounded crowd.

88. While the technical difficulty of verification should not be exaggerated, its importance cannot be overstated. If used by a human rights organization, unverified material can lead to the degradation of the organization's credibility, but hoaxes can also create combustible situations – so-called "digital wildfires" – that can lead to violence.[72] Many States already have laws limiting freedom of expression for reasons such as incitement of violence or panic, but they are struggling with how to apply those laws effectively to online activities. Any regulation in that area will remain complex and controversial; it has been suggested that the online community itself must fill the gap, with important roles for community curators and moderators.[73] The Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance reported to the Human Rights Council in 2014 on the complex challenges for his mandate posed by the Internet and social media (A/HRC/26/49). In addition to pointing out policies developed by some of the major social media sites, he also highlighted the importance of civil society initiatives.

4. Using digital evidence

89. Most of the information that can be captured through the streams described above is "convenience data", but its value to a human rights investigation cannot always be immediately

67 See, for example, the Rashomon Project, http://rieff.ieor.berkeley.edu/rashomon/about-rashomon/.

68 Craig Silverman (ed.) *Verification Handbook: An ultimate guideline on digital age sourcing for emergency coverage* (European Journalism Centre, 2014), http://verificationhandbook.com/.

69 See "A field guide to enhancing the evidentiary value of video for human rights", http://verificationhandbook.com/book/appendix.php.

70 Ella McPherson, "Digital civilian witnesses of human rights violations: easing the tension between pluralism and verification at human rights organizations" in Lind (ed.), *Producing Theory 2.0: The Intersection of Audiences and Production in a Digital World*, vol. 2 (forthcoming 2015).

71 See Victor Naroditskiy, "Veri.ly – getting the facts straight during humanitarian disasters", (August 2014), www.software.ac.uk/blog/2014-08-13-verily-getting-facts-straight-during-humanitariandisasters.

72 This issue was raised in the World Economic Forum Global Risks report, 8th ed. (2013), pp. 23–27.

73 See Lee Howell, "Only you can prevent digital wildfires" *New York Times* (8 January 2013), available at: www.nytimes.com/ 2013/01/09/opinion/only-you-can-prevent-digital-wildfires.html.

assessed. Moreover, it is important not to privilege images as much can also be learned from blogs or micro-blogs, which can be used to corroborate other sources.

90. While verification subsidies potentially speed up the verification process, using them requires digital literacy about verification among human rights fact-finders and civilian witnesses. It is unclear how knowledge about producing and transmitting information effectively, safely and ethically for evidence will be diffused among civilian witnesses, particularly those who are acting in a truly spontaneous manner. Pre-emptive steps to train human rights monitors will favour the prepared, but it is often the accidental witnesses who are best placed to be truly informative.

91. For that reason, organizations such as WITNESS advocate for the standard inclusion of an "eyewitness" or "proof" mode, resembling InformaCam, in preloaded photo and video applications on smartphones and in social media platforms.[74] The inclusion of those features in mainstream applications and platforms means that civilian witnesses are more likely to know about them and thus to use them.

F. Use of information and communications technologies by human rights mechanisms

[...]

2. National and international commissions of inquiry

100. Various national investigations have made use of digital evidence. The finding that the death of Ian Tomlinson during a demonstration in London in 2009 was an unlawful killing hinged on a witness video that was tracked down and handed over to the Independent Police Complaints Commission by an investigative reporter. Also, the ongoing inquiry into the shootings at Marikana, South Africa, received ostensibly probative video evidence that the South African Human Rights Commission has had synchronised by a technological expert.

101. At the international level, OHCHR has partnered with the Operational Satellite Applications Programme of the United Nations, and with various external partners on an ad hoc basis, to use both satellite and video evidence in the work of international commissions of inquiry. As discussed above, when combined with other techniques of human rights monitoring, satellite imagery can provide extremely valuable information for inclusion in reporting to the Human Rights Council.

102. The Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea made use of both satellite imagery and clandestinely recorded videos and photographs in order to demonstrate the existence of several political prison camps (see A/HRC/25/63). The Commission relied on the videos and photographs to the extent that they could confirm their authenticity, and, with respect to satellite imagery, on commercially available footage. The Commission noted that higher resolution satellite imagery produced by more technologically advanced States would, almost certainly, have provided further information. Unfortunately, despite requests, those images were not made available to the Commission (see A/HRC/25/CRP.1, para. 60–61).

103. The Independent International Commission of Inquiry on the Syrian Arab Republic has also made use of a certain amount of satellite and digital material, as one might expect from a body monitoring one of the most documented conflicts in history. In conducting its special inquiry into the Al-Houla killings, for example, the Commission examined satellite imagery to review access points to an area where killings had occurred, as well as to review statements made by interviewees and to assess claims that the Government had razed civilian areas in Damascus and Hama. The Commission mentioned instances where it had received or found video evidence supporting

74 Sam Gregory "How an Eyewitness mode helps activists (and others) be trusted", *WITNESS Blog* (3 March 2014), http://blog.witness.org/2014/03/eyewitness-mode-helps-activists/.

allegations of torture or other forms of illtreatment or footage of killings, but noted when it could not verify those recordings. Video material has also been directly gathered by the United Nations Supervision Mission in the Syrian Arab Republic and referred to in reports of the Commission. The Commission also undertook preliminary reviews and conducted forensic analyses of 26,948 photographs allegedly taken between 2011 and 2013 in government detention facilities. In more recent reports, the Commission cited a number of videos that had been created and distributed by ISIS; those videos have been a challenge to the current methodology of using videos only to substantiate events for which there are other witness testimonies, but the Commission has given them weight as confessions.

3. International criminal accountability

104. Information derived from digital sources has become increasingly important to international tribunals, including several of those established during the 1990s, and now also the International Criminal Court. In assessing the importance of such evidence to moving forward its work, the Court has been proactive in establishing working methods that can accommodate such evidence. In 2012 and 2013, the Court encouraged partners to exchange ideas and expertise on strategies to improve the capacity of investigators and prosecutors to gather and analyse digital evidence concerning serious international crimes.

105. One of the recommendations from that process was that the Office of the Prosecutor should "hire specialists trained in advanced cyber-investigation techniques and familiar with cutting-edge technologies" and who would have "experience and credentials specific to digital investigations, including computer and smartphone forensics, online investigations, data storage and management, advanced cyber-investigation techniques, and superior knowledge of digital security." It was suggested that this would "go a long way toward building a robust in-house capacity for vetting digital data and extracting quality evidence." On the basis of that consultation, the Office of the Prosecutor appointed a specialist in the verification of digital material to work as a "cyber-investigator", as part of its team of other investigators from legal and law enforcement backgrounds.

106. Recognizing the transient nature of much of the relevant material, the Office of the Prosecutor has adopted the practice of surveying digital evidence that is available when the preliminary examinations are opened. As noted above, the Court has developed guidelines for use by investigators concerning best practices with respect to the retrieval, storage and investigation of digital evidence, including the capture of websites and seizure of hard drives.

The Minnesota Protocol on the Investigation of Potentially Unlawful Death (2016) (see Chapters 2 and 9) also provides extensive guidance to investigators on the treatment of digital evidence.

The Minnesota Protocol on the Investigation of Potentially Unlawful Death (2016): The Revised United Nations Manual on the Effective Prevention and Investigation of Extra-legal, Arbitrary and Summary Executions (2017, ¶¶78-80, 143-145)

B. The Investigation Process

[...]

7. Telecommunications and other digital evidence

78. Within the confines of the applicable law, mobile telephone data should be requested from service providers. This information may help in establishing the identity, roles and relationships of persons of interest and their presence and participation in key activities (such as presence at

key locations, attendance at meetings, the conduct of any surveillance, the procuring of materials and the execution of the crime). In planning an investigation, investigators should familiarise themselves with the data-retention policies of the service providers. Mobile phone data allows authorities to analyse the phone numbers that connect to a particular phone tower within a given period of time. Investigators can then match the mobile phone numbers with a particular customer's name, address and other account information, potentially putting individuals at locations at specific times. The mobile phones of the deceased and all prime suspects should be legally recovered and relevant data (e.g. dialled, missed and received calls, text (sms) or other messages, photographs, contacts and diary entries) professionally downloaded. The phones can then be returned to the family of the deceased or to the suspect, as the case may be. Where a phone is recovered that appears to have been used by a perpetrator, but the identity of the user or owner of the phone is not otherwise established, service provider or other information showing that the recovered phone has made or received calls or messages from family members of a prime suspect will make it easier to demonstrate, using phone attribution analysis, that the phone belonged to or was used by a particular suspect.

79. For all phones identified as relevant it may also be useful to request subscriber details, method of payment and call data, together with mobile phone site locations and any other data providers can offer. This may include text messages or International Mobile Station Equipment Numbers, which may identify the type, model and capability of the handsets used. Smart phones used by the victim or any suspects should be analysed for Wi-Fi locations activated and Internet sites visited for information which may provide leads in the investigation. Where possible, investigators should also obtain cell site coverage maps from service providers.

80. Analysis should compare call-data numbers and data, cross-referencing the movements of all people of interest in the case, on pictorial charts using specialist software, if available.

[...]

F. Types of Evidence and Sampling

[...]

4. Digital evidence

143. Digital evidence is information and data that are stored on, received from or transmitted by an electronic device. Digital evidence can be found in images on cameras, on the internet, computers, mobile phones and other digital media, such as USB sticks.

144. Digital evidence has become increasingly important in investigations. It can be recovered from a number of sources: open systems such as the internet and social media; and closed systems such as computers, laptops, mobile phones and cameras. Internet and mobile-phone service providers frequently keep their data (e.g. call records) for only a limited time. In planning an investigation, investigators should be aware of how long data is retained by these providers so they can ensure that the appropriate information is requested within the available time frame.

145. Digital information can be recorded in various formats: photographs, audio recordings, video recordings, email/network communications, text/sms messages, mobile phone applications and social media. All of this information can be useful to an investigator. The metadata (e.g. information on the creator, date of creation, device, location, alteration/changes) can provide valuable information. However, this metadata can also be easily manipulated. Authenticating digital evidence is a technical challenge. If digital evidence is considered to be important in an investigation, every effort should be made to ensure that a qualified forensic expert recovers and/or examines the evidence.

One of the first prominent examples of the use of ICTs in the work of the Special Rapporteurs was the emergence of video footage that appeared to depict summary executions by the Sri Lankan government during its conflict with the Liberation Tigers of Tamil Eelam. Controversy erupted when the Government of Sri Lanka contested its legitimacy. The series of letters exchanged by Special Rapporteur Alston and the Sri Lankan government is extracted in Chapter 9. Below is an extract from a technical report prepared by Special Rapporteur Heyns, relying heavily upon expert advice, in which he addressed some of the claims being made by the Sri Lankan government.

Summary of information, including individual cases, transmitted to Governments and replies received (A/HRC/17/28/Add.1, 27 May 2011, Appendix I §§1-41, 45)

A. Technical Note by the Special Rapporteur on extrajudicial, summary or arbitrary executions, Mr. Christof Heyns, in relation to the authenticity of the second, extended Channel 4 videotape regarding Sri Lanka

A. Background

1. On 30 November 2010, the UK television station Channel 4 made available video material of around five minutes in duration (in this note called the 'extended video') to the United Nations Special Rapporteur on extrajudicial, summary or arbitrary executions, Mr. Christof Heyns. It described this video, extracts of which had been aired by Channel 4 around the same time as a longer version of an earlier video of approximately one minute (in this note called the 'first video'), which was aired by Channel 4 on 25 August 2009 and was said to depict Sri Lankan soldiers summarily executing Tamil prisoners during the civil war in that country.

2. The first video has been the subject of extensive communication between the Government of Sri Lanka ('the Government') and the former Special Rapporteur Mr. Philip Alston, in the form of an exchange of letters and press releases, as well as a 'Consolidated Response' to the Channel 4 video by the Government and a subsequent 'Technical Note' by Mr. Alston.

3. In reacting to the screening of this video by means of a letter of allegation to the Government of Sri Lanka, Mr. Alston's contention was that the video necessitated an impartial investigation into the question whether war crimes had been committed. The Secretary-General of the United Nations as well as other diplomats also expressed their concern about the contents of the video. The Government, however, denied the authenticity of the video.

4. In order to support this contention, the Government presented a 'Consolidated Response' to the media and the diplomatic community. It cited four reports of investigations into the authenticity of the video which the Minister of Disaster Management and Human Rights said it had obtained from its experts. While those cited seem to be regarded by the Government as experts in the field of video and audio technology, the Government also relied on their opinions on matters of forensic pathology and ballistics. According to the Minister these reports proved that the video was 'false and fabricated'. The claim was made that the Government's investigations proved that the recording was not made on a cell phone, as stated by Channel 4, but on a high quality digital camcorder or similar equipment, and then edited to reflect the atrocities and to make it appear to have been made on a cell phone, in order to discredit the Government.

5. Mr. Alston commented that he had not seen the original version of three of the four reports and asked to see them. Mr. Alston also questioned the impartiality of those who conducted the investigation, pointing out that two of the four were members of the armed forces (one was a Major, the other a Brigadier), the body which actions have been called into question, and the other two were apparently also citizens of Sri Lanka who had previously acted as advisers to the Government.

6. Mr. Alston then commissioned a study of his own by three independent experts with no links to the country or government under consideration. In addition to a video and audio expert, he engaged the services of a forensic pathologist as well as a ballistics expert, who worked independently of one another. They contested the scientific nature of the comments attributed by the Government to its own investigators. On the basis of these reports Mr. Alston concluded that 'while there are some unexplained elements in the video, there are strong indications of its authenticity.' He made the full reports available to the Government.

7. In its subsequent reactions, the Government has relied on these 'unexplained elements', clearly acknowledged by the Rapporteur, to contest his claims that the video was authentic and to justify rejection of his continued calls for an independent investigation.

8. In particular, the following issues were identified as unexplained: The date inscribed on the video was after the hostilities had ceased; there is an 'A' in the last 17 frames of the video, which suggests that some editing had been done; one victim's leg remains upright after he has apparently died; and another's dead body moves without an apparent reason

9. It appears from the record of communication between the Government and the Special Rapporteur that the Government's contention regarding the first video is confined to the question whether the video is authentic or 'doctored' or 'a fake'. Issues such as whether the members of the military depicted in the video wear Sri Lankan uniforms (except for one soldier who wears a white T-shirt) and whether they speak Sinhala (this is in fact recognised in the excerpts of the report provided by Maj Bandara) or for that matter whether the setting of the video is in Sri Lanka, are apparently not contested. It is also not contested that the actions depicted in the video, if they reflect real events, constitute serious international crimes and violations of international human rights law. While the independence of those whom the Government say have written reports for it has been questioned by the Special Rapporteur, the independence and expertise of the experts engaged by the Special Rapporteur has not been placed in doubt.

10. The single point of contention that has emerged from the intensive communication over several months between the Special Rapporteur and the Government is therefore the authenticity of the first video, in the sense that the Government contends that it had been 'doctored'.

B. The new, extended video

11. On the extended video additional executions are shown, as well as bodies that lie on a track of ground. The faces of some of the soldiers are visible. Also clearly visible is that others are filming the scene with cell phones. One of the voices on the extended video says: 'Do not use the phone, we will be reprimanded.'

12. The extended video offers the opportunity to see the first video (which forms one segment of the extended video) in a broader context, and in particular to test the results of the earlier investigations, to see whether anything stated by the independent experts has been disproved by this new video, and whether answers to the unexplained issues may be provided by the new material.

13. I as Special Rapporteur, who took over the mandate from Mr. Alston in August 2010, informed the Government on 15 December 2010 that I would be investigating the extended video. Upon request from the Government I informed of the names of the experts who have been commissioned to conduct the investigation, and the Government was supplied with a copy of the video as received from Channel 4, to enable it to do its own investigation.

14. In view of the fact that the expertise and independence of the experts who investigated the first video was not questioned by the Government, and the fact that they were already familiar with

part of the material, the services of the same experts were again obtained, to comment within their fields of expertise on the authenticity or falsity of the video. As in the past they agreed to do this free of charge, as a form of public service.

15. In addition, some further evidence was obtained and considered by the current me that would be useful in better understanding the context of the video. This included a translation of what is being said in the video, from the original Sinhala. A large number of additional pictures and other material were received from NGOs who have concerns surrounding these events. However, as will be explained below, the latter were not investigated in any detail by me.

16. Enquiries were also made by me about the origins of the video from Channel 4. However, given that the video was more than likely filmed by an insider, and then made available to the media (whether this was done for compensation or not is not known), it is not a surprise that the journalists in question maintain that they have obtained the videos on the conditions of confidentiality from their sources. While such information would no doubt be very useful in any subsequent criminal trials, not least because it would provide one with an eye-witness of the events who could identify those involved (also those not seen on the video) it is not regarded as indispensable for current purposes, which is simply to ascertain the authenticity of the video itself.

17. The authenticity of a video such as the one under consideration can be established through a comprehensive forensic investigation, covering the different aspects of the video, which should include at least the audio and video quality. Forensic pathologists and ballistics experts can also contribute in important respects to such an investigation. In order to be credible such investigations have to be conducted by independent people of recognised expertise. Independence in this context, according to well-established jurisprudence means there should not even be a perception of bias. Close connections to the Government or State under consideration – such as nationality and/or employment – are bound to create a perception of bias and a perceived conflict of interest.

18. The new reports of the three experts on the extended video provided to me are attached. The picture that emerges is that the events that are reflected in the video in fact occurred as depicted. These videos – both the first and the extended version – show real people who are being summarily executed.

19. The first report on the extended video, contained in Annexure 'A', is by audio and video expert Mr. Jeff Spivack. His qualifications and experience are detailed in his report, as was the case with his previous report.

20. According to his report the extended video in fact consists of five segments, not in chronological sequence. This appears to be the result of the rudimentary editing that is possible on a cell phone. In this case the meta-data indicates the use of Philips software, which can be used on a variety of cell phones. However, cell phone editing capacity could not have been used to produce the images of executions captured on the video. 'At most, integrated mobile phone editing software could delete evidence that occurred before or after the remaining video, or reorder video sequences.' Cell-phone editing '… could not possibly create even a crude simulation of the subject matter present in these recordings, much less a realistic simulation.' (p 13)

21. He concludes that '… the results of testing procedures and content analysis are persuasive that the events depicted on the available video/audio recordings are authentic.' (p 13)

22. The second report, contained in Annexure 'B', is by Mr. Daniel Spitz. His biography and expertise are also described in his report. His conclusion upon having studied the extended video is as follows: 'Subsequent to my review of these materials, it is my opinion that the execution shootings shown in the videos represent real executions of multiple individuals secondary to close range gunshot wounds using high powered assault rifles.' (p 1)

23. The third report, contained in Annexure 'C', is by Mr. Peter Diaczuk, a firearms evidence expert, who comments on the three clips in the extended video where firearms are being discharged. His experience and training is indicated in his report. His conclusion is as follows: 'The three video sequences reviewed accurately depict firearms being discharged, and the recoil observed is consistent with the firing of live ammunition.'(p 4)

24. Of special importance is the fact that the extended video material has now enabled the experts to address the issues identified as 'unanswered' during the first round, and relied upon by the Government as proof that the video was not authentic.

25. The date of 15 (alternatively 18) July 2009 is encoded in the video, while hostilities had ceased in May 2009. One explanation is that the date provided on such a video is determined by the device's date setting, which can be changed by the person using the device. However, according to Mr. Spivack, if the rudimentary editing that is possible on a cell phone is done, and if five segments are put together as we now know was the case here, the date reflected for the video as a whole will be the date of such editing. (p 7)

26. The appearance of an 'A' in the last 17 frames of the first video was also a matter of concern. According to Mr. Spivack the rudimentary editing possible on a cell phone can produce such an effect. (p 13)

27. It was previously unclear why one of the apparent victims on the ground next to a victim being shot shows movement of his left lower extremity. However, Mr. Spitz reports that from the extended video it is clear that the bullet passed through the one person to hit the body of the other (p2).

28. The way in which the leg of one of the victims was maintained in an upright position was likewise not readily explicable when only the first video was available. Dr Spitz now explains that a review of the current video 'better shows the position of the leg and why it maintained an upright position'. The reason is that '… the ankle is supported by resting against the outer aspect of his right leg.' (p3)

29. The integrity of the process followed by these experts in respect of the first video finds confirmation in the fact that they marked certain aspects of that video as unresolved, when they did not have sufficient evidence to express themselves on those points. This uncertainty has now been resolved on the basis of the newly available evidence, which could not have been foreseen at the time when the first reports were being written. The above sequence of events show that they were describing the facts as they presented themselves, and were not out to prove any point.

30. The above serves as a coherent and credible foundation for the conclusion that the extended video is authentic, and thus warrants calling for the accountability of those responsible for these atrocities. It should be stressed however that the claim is not being made here that any specific individuals are guilty or that State responsibility has been established – the point is rather that there is a well-founded case for the government to answer.

31. Reference was made in the Technical Note of Mr. Alston to an article in The Times newspaper where an expert, whom it had commissioned, Grant Fredericks, also regarded the first video as authentic.

32. The Government told the Office of the High Commissioner for Human Rights in Geneva, when it was provided with the names of the experts who were going to investigate the extended video, that it would be more persuasive if a report by someone who was not part of the team of Mr. Alston during his investigation were made available. Because the independence of these experts was not challenged by the Government when their first reports were considered, it is hard to see

the foundation for this point. However, to err on the side of caution, the current writer has asked Mr. Fredericks as well to do an independent investigation into the extended video. His report is attached as Annexure 'D'.

33. Mr. Fredericks – whose credentials are set out in his report – is of the opinion that Phillips software was used, probably on a Nokia cell phone to make the extended video. (p28) He concludes as follows: 'Giving consideration to my research and to the observations listed in this report, I have found no evidence to suggest that [the extended video] contains fabricated images or audio elements. The execution scenes contain no 'virtualization' (computer generated effects). I have therefore formed the opinion that [the extended video] is authentic in that it accurately portrays what it purports to show.' (p 29).

34. As was noted at the outset, the current Special Rapporteur was provided with numerous pictures and other material said to depict the last phases of the civil war in Sri Lanka. Sources at Channel 4 have also indicated that a much longer version of the extended video exists and could become available. The material that has already been provided includes pictures and videos of a Tamil journalist named Isaipiriya who bears a striking resemblance to one of the persons whose dead body is captured in the extended video. The material also includes pictures of the dead body of Charles Anthony (son of the late LTTE leader Prabhakaran) who was killed during the final phases of the war, in a group of pictures containing one that corresponds with images captured in the last section of the extended video. Channel 4 has also provided the Special Rapporteur with a video that captures the removal of the naked bodies of women by soldiers, said to be government troops. On this video – as is the case with the extended video – the faces of those in uniform can clearly be seen, and soldiers using cell phones as cameras are also visible.

35. These and other links with the extended video have so far not been investigated in any detail by the Special Rapporteur, in view of the limited nature of his capacity for factfinding and forensic investigations. In view of the serious nature of the material covered by the growing body of potential evidence, it should be investigated by a body with the necessary capacity to do a comprehensive, thorough study. The material mentioned above will be made available to the Government upon request, and to such an international body, in order to assist any credible enquiry.

36. There is no indication at present that either the Attorney-General, or internal structures within Sri Lanka, such as the Lessons Learned and Reconciliation Commission, have given serious consideration to this video, or its implications, in their work.

C. Conclusion

37. The present note confines itself to the question of the authenticity of the extended video, based on the results of the independent, multi-disciplinary forensic studies that have been commissioned. The conclusion that emerges from these reports is that the video is authentic.

38. The outstanding issues identified during the investigation of the first video have now been resolved. This includes the apparent inconsistent date on the first video. However, even if that had not been done, the question could be asked how material that issue was in the first place. If someone had manufactured a false video of the events during the final stages of the war, with the malicious intent of portraying the Government's conduct during the war in a negative light, the last thing one would expect such a person to do is to provide the video with a date that falls months after the completion of the war. Likewise, it appears highly unlikely that a person who wants to create the impression that a cell phone was used would be so careless as to leave an 'A' on the frames if that can only be done on a high quality video camera. However, irrespective of how much weight could legitimately have been accorded to these issues, it is submitted that they have now been resolved.

39. On the basis of the available evidence the process of determining accountability for the crimes that have been committed should proceed with sufficient speed to avoid a situation where witnesses, accused or evidence disappear.

40. The extended video should be considered in the context of the growing body of evidentiary material which appears to relate to the events during the civil war in a comprehensive manner, covering possible atrocities by all concerned, by an institution with the necessary capacity and level of technical skill to cover such an extensive enterprise in a professional and comprehensive manner, on the basis of a clear mandate to perform this function.

41. What is reflected in the extended video are crimes of the highest order – definitive war crimes. Judging by the use of cell phones by soldiers in the video, there may well be other records of the same events available. There appear to be links that can be made to other evidentiary material, which is already available or may still be brought to light, giving a clearer picture of what happened during the last phase of the war. Investigating the identity of those whose faces are captured so clearly on these videos cannot be difficult for the Government, which may contact the commanders of the troops who participated in the last phases of the war. Similarly, an international investigation with appropriate powers of inquiry and witness protection

[...]

45. In conclusion, what has been said above should be re-emphasised, to avoid any misunderstandings: This note does not purport to find the Government or any of its agents guilty of any offence. This can only be done by a court of law. Instead, the claim is made here that the extended video provides credible evidence that serious crimes have been committed within the context of the Sri Lankan civil war, which should together with any other available evidence be examined systematically and professionally by domestic investigators, as well as by an independent, international investigational body, with a clear mandate in this regard, in order to establish who should be held accountable for these coldblooded killings.

5. Use of ICTs by human rights mechanisms

This chapter has largely dealt with the use of ICTs by civilian witnesses, activists, and governments in their accountability efforts. However, ICTs are also available to various intergovernmental human rights mechanisms, including the Human Rights Council and its Special Procedures. As Special Rapporteur Heyns discussed in 2015, these mechanisms are sadly lacking in ICT expertise.

Report to the Human Rights Council (A.HRC/29/37, 24 April 2015, ¶¶93-99, 107-111, 114-116)

93. The broader United Nations community has invested in harnessing the potential of ICTs, particularly in the area of crisis information management (A/69/517). The United Nations Office of Information and Communications Technology has, in conjunction with the ICT4Peace Foundation, coordinated the Crisis Information Management Advisory Group, which has become a forum to discuss technological developments in humanitarian aid and crisis information management.[75] The Office for the Coordination of Humanitarian Affairs (OCHA) has reviewed the impact of ICT-enabled networks on humanitarian relief and has, since then, undertaken a

75 See http://ict4peace.org/crisis-information-management-advisory-group-cimag-retreat/.

number of collaborative projects to take advantage of the power of the crowd.[76] Meanwhile, the Global Pulse project is a major undertaking on the humanitarian impact of big data.[77]

94. In 2014, the Department of Peacekeeping Operations requested the Expert Panel on Technology and Innovation in United Nations Peacekeeping to recommend ways in which technology and innovation could enhance their operational effectiveness. The panel issued its final report in February 2015,[78] in which it recommended that, among other things, the Security Council create a special technical mission to use technical audio, visual, monitoring and surveillance technologies to inform decision-making.

95. The United Nations human rights mechanisms have not completely ignored the advances of ICTs. Several of them have created successful social media presences as part of their promotional engagement strategies and campaigns to reach millions of users worldwide. Although the promotional uses of digital ICTs are significant, the Special Rapporteur will now consider the engagement of various international and regional human rights mechanisms that use ICTs for fact-finding and accountability.

1. Special procedures and other mechanisms of the Human Rights Council

96. This report was in part motivated by the Special Rapporteur's investigation of video evidence of executions at the end of the civil war in Sri Lanka (see A/HRC/17/28/Add.1, appendix). In that instance, the Special Rapporteur was able to provide impetus to a broad coalition pressing for accountability by independently seeking out technical experts to comment on the metadata of the videos, the ballistics of the weapons shown in the videos and the movement of the bodies. Given the rapid developments in the field, it is quite possible that such expertise is easier to find today, however, the capacity of OHCHR has not changed greatly. Special procedures mandate holders would benefit from in-house technical knowledge for selecting the best experts for specific tasks.

97. As noted above, the verification of user-generated content is fundamental to reaping the advantages of ICTs in terms of broadening access to and the scope of human rights work. However, it is important that verification not be viewed as a barrier to the use of digital evidence. The technical difficulty of verification is sometimes exaggerated and used as an excuse not to engage with such evidence. Verification should be demystified within the international human rights machinery, so that the advantages offered by digital evidence can be more fully embraced.

98. With respect to the dangers of ignorance concerning digital security, it is noteworthy that many Human Rights Council mechanisms encourage individual contact through insecure generic email addresses, with no warnings concerning security or suggestions of alternatives. While offering such contact points is a laudable effort to broaden access to its mechanisms, the Council is arguably failing in its duty of care by failing to adequately warn individuals or groups of the potential risks that they may be taking.

99. Of course, the impression should not be given that the special procedures of the Council are closed off to information from the new data streams discussed in the present report. Indeed, much of the NGO reporting on which special procedures' communications are based derives information from such sources. However, the fact that the Council is not yet open to weighing such evidence or reporting places it at risk, over the coming years, of isolation from the broader human rights community with which it has done so much to engage in the past.

76 OCHA Policy and Studies Series, Humanitarianism in the Network Age: including world humanitarian data and trends 2012, (2013), https://docs.unocha.org/sites/dms/Documents/ WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

77 See http://www.unglobalpulse.org/.

78 See http://www.performancepeacekeeping.org/offline/download.pdf.

[...]

Conclusion

107. ICTs have had a profound effect on the impact and character of human rights work. However, it is important that the process not be taken too far, especially in information-scarce environments, where it will be increasingly important to resist the temptation to privilege digital material. While new technology may raise expectations for information, it should be noted that traditional human rights monitoring and reporting make no claim to comprehensiveness, and neither should analysis of new ICT-enabled data streams. The latter should not be viewed as a shortcut, but rather as part of a complementary process that fits into pre-existing strategies used by human rights actors.

108. It is also important that ICTs be embraced with due acknowledgement of their risks. While in many cases, technology can be a vehicle for pluralism, issues of a digital divide remain. In order to benefit from digital protection measures, human rights defenders need to know about them. The digitally enabled promotion of human rights may contribute to a culture of awareness, but if promotion resources for those initiatives are diverted away from more traditional channels, this will be to the detriment of vulnerable groups who are not online.

109. It is also important to acknowledge the importance of ownership and control of the mechanisms of digital ICTs. The use of digital evidence often depends on the willingness of technology corporations to host, store and facilitate searches for this information. Moreover, in some States, access to externally owned commercial social media platforms, such as Twitter, Facebook and YouTube, are blocked. In others, entire communication networks have been shut down to suppress the flow of information.

110. Keeping up with digital literacy and paying for new technology can be difficult for human rights organizations. One solution would be collaboration between ICT specialists and human rights experts to develop, implement and even commercialise new applications for human rights, or to negotiate low-cost or free licensing for the use of existing solutions. Donors are interested in funding technological developments, but reportedly can focus more on the technology than on the training that is required to deploy it. However, technology can be useless or even dangerous without training. As one observer noted, "sooner or later, all technology problems become education problems."[79]

111. The collaborative framework can be extended further. Indeed, a wide range of organizations are willing to assist international human rights mechanisms in more fully benefiting from ICTs. Coordination efforts have been made in that regard, but it seems that the human rights community is currently far behind other international agencies – most notably in terms of crisis response – in fully realizing that potential.[80]

79 Christopher Neu, "Mobile applications for atrocity prevention require mobile students", *TechChange*, (19 February 2013), available at: http://techchange.org/2013/02/19/mobile-applications-for-atrocity-prevention-require-mobile-students/.

80 In the humanitarian response context, Digital Humanitarian Network has produced two reports aimed at both sides of such partnerships: see http://digitalhumanitarians.com/content/guidance-collaborating-formal-humanitarian-organizations, and http://digitalhumanitarians.com/content/guidance-collaborating-volunteer-technical-communities.

Recommendations

To the United Nations

114. OHCHR should appoint, on a consultancy basis and as soon as possible, a digital content specialist to provide advice with respect to information received from or produced by civilian witnesses and to serve as an interface with external networks of expertise in that area. That should be seen as a stopgap solution to ensure quick movement on that front. At the same time, OHCHR should, with the assistance of the appointed specialist, set about establishing longer-term capacity.

115. As international commissions of inquiry and fact-finding missions are ad hoc bodies that are likely to receive a large and increasing quantity of digital evidence, consideration should be given to expertise for analysing such material in the staffing requirements for those mechanisms.

116. More broadly, OHCHR should take steps to improve awareness of and to familiarise its staff and processes at all levels with the requirements of digital security. That involves the development of minimum standards of due diligence with respect to the digital security of sources. Guidelines for United Nations staff on the ethics of using information from open sources, especially social media, should also be developed in consultation with relevant partners.