

The Future of Human Rights Technology

A Practitioner's View

Enrique Piracés

I INTRODUCTION

Technology has been extraordinarily effective in reducing distances between people and places, but it has created an increasing distance between the present and the future. The rates of new product introduction and adoption are speeding up. It took forty-six years for electricity to reach 25 percent of the US population. The same milestone took thirty-five years for the telephone and only seven for the Internet. For most of us, it is increasingly difficult to understand or anticipate long-term technological trends. It is common, especially in the context of human rights practice, that such inability stokes fears of a dystopian future in which ordinary people, especially those already marginalized or disenfranchised, become subjugated by technology rather than benefiting from it. This chapter is both an attempt to help practitioners cope with new technologies and a proposal to incorporate solidarity as the driving force for technology transfer.

It has become cliché to say that technology and its impact on society advance at a rapid pace. It is also commonplace to say that societies and legal frameworks have a hard time adapting to technology's pace and the behavioral changes it demands. But adaptation is a valuable goal, because there is no livable future without it. The human rights movement has taken note and, both systematically and spontaneously, looked for ways to adapt to the transformative era of the information society. Today, human rights campaigns rely heavily on social media and e-mail. The presentation of research results in courts, political offices, and public spaces commonly incorporates data visualization. Fact-finding practices often include the use of remote sensing and open source intelligence. Further, human rights research increasingly relies on computational analysis. Encrypted communications, and the tools and services that provide them, are now considered fundamental to the safety of human rights practitioners and their partners in the community. These are signs that, as the contributors to this volume remind us, the future of human rights will be intertwined with the advancement of technology.

The pace of technological change is unlikely to slow, and its relevance for human rights practice is unlikely to diminish. There is a valuable body of work, created over the past few decades, that focuses attention on the impact of technology on human rights. The lessons that we can extract from that literature will enrich our design for the future as well as our ability to evaluate the present.¹ Yet, as Molly Land and Jay Aronson point out in Chapter 1, the field of human rights technology is significantly undertheorized. I would add that the relationship between practice and theory has garnered even less attention. The contributors to this volume have gone a long way to redressing the first issue, especially with respect to human rights law. If we are to solve the second challenge, however, practitioners must help frame the debate in this interdisciplinary field. Doing so is essential to the advancement of effective human rights practice.

II WHERE DOES THE FUTURE BEGIN?

Over the past ten years, the notion of human rights technology as an area of practice has garnered attention across disciplines. The growing use of the term “human rights technology” signals the interest of technical, scientific, and practitioner communities in advancing it as a field of practice. An important example, and one of the likely origins of this multidisciplinary interest, occurred in 2009, when the Human Rights Center at the University of California, Berkeley called for “leading thinkers, civil society members, activists, programmers, and entrepreneurs to imagine, discover, share, solve, connect, and act together.” This invitation materialized as an international conference, “The Soul of the New Machine: Human Rights, Technology & New Media,”² held in May 2009, and a follow-up conference, “Advancing the New Machine: A Conference on Human Rights and Technology,”³ held in 2011, both in Berkeley. A diverse mix of academics, practitioners, and technologists attended those events, which launched a constructive debate about the uses of technology for human rights practice.

Since then, a growing number of efforts to create dialogue, promote debate, and engage technologists with rights defenders have emerged across the globe. Strategic donors to the human rights movement, like the MacArthur Foundation, the Ford Foundation, the Oak Foundation, Humanity United, and the Open Society Foundations, amplified these efforts. These foundations adapted their portfolios to help create the human rights technology field. Governments have also played a role,

¹ C. Weeramantry, *The Impact of Technology on Human Rights: Global Case-Studies* (Tokyo: United Nations University Press, 1993); J. Metzl, “Information Technology and Human Rights” (1996) 18(4) *Human Rights Quarterly* 705–46; R. Jørgensen et al., “ICT and Human Rights” (FRAME Deliverable No. 2.3, 2015).

² “Soul of the New Machine,” UC Berkeley School of Law, www.law.berkeley.edu/research/human-rights-center/past-projects/technology-projects/soul-of-the-new-machine/.

³ “Advancing the New Machine: A Conference on Human Rights and Technology,” UC Berkeley School of Law, www.law.berkeley.edu/research/human-rights-center/past-projects/technology-projects/advancing-the-new-machine-a-conference-on-human-rights-and-technology/.

as can be seen in the programming of the Bureau of Democracy, Human Rights, and Labor at the US State Department,⁴ the Open Technology Fund⁵ of Radio Free Asia (an initiative of the US Broadcasting Board of Governors), and the Swedish International Development Agency.⁶

By now, there are dozens of international, regional, and national conferences and workshops each year that include debates on the use of technology for human rights.⁷ Many organizations, like Benetech, HURIDOCS, and eQualit.ie, have carved a niche providing specialized technology and support to human rights practitioners. The growing interest can also be seen in the appearance of specialized and globally distributed communities of practice around issues of technology and human rights, such as the Internet Freedom Festival,⁸ held yearly in Valencia, Spain, since 2015. This interest in technology has also reached traditional international actors like Amnesty International and Human Rights Watch, which have pioneered specialized programs within their organizations to address their remote sensing, data analysis, and digital security needs.⁹ These examples are evidence of the growing and vibrant ecosystem interested in applying technology to solve human rights problems.

In order to frame how we think about the future of this field, it is essential to be aware of our own geopolitical and cultural positions. Human rights technology has not escaped some of the persistent problems that have faced the broader human rights movement. The most obvious, perhaps, has been the tendency to consolidate power in the economic capitals of the twenty-first century, geographically removed from most human rights crises. This can be acutely felt in the realm of technology, where investment in infrastructure can be too costly for grassroots organizations in the Global South. Current models of technology transfer reflect a unidirectional relationship, where technology is largely decided, designed, and created far away from the majority of people who need it. As Dalindyebo Shabalala reminds us in Chapter 3, funding and enforcement mechanisms for providing access to technology remain a challenge for effective technology transfer in international cooperation for adaptation to climate change.

⁴ “Internet Freedom Funding Opportunity: State Department’s Bureau of Democracy, Human Rights, and Labor (DRL),” Open Technology Fund, www.opentech.fund/article/internet-freedom-funding-opportunity-state-departments-bureau-democracy-human-rights-and.

⁵ “About the program,” Open Technology Fund, www.opentech.fund/about/program.

⁶ “The Access Grants Program – an emerging initiative,” Access Now, June 25, 2015, www.accessnow.org/the-access-grants-program-an-emerging-initiative/.

⁷ “RightsCon Summit Series, www.rightscon.org/about-and-contact/; Y. Ulman, *Report on the International Conference on “Emerging Technologies and Human Rights” Council of Europe Bioethics Committee, DH-BIO, Strasbourg, 4–5 May 2015* (December 2015).

⁸ “History, Goals and Guiding Principles,” Internet Freedom Festival, <https://internetfreedomfestival.org/history/>.

⁹ “Remote Sensing for Human Rights,” Amnesty International USA, www.amnestyusa.org/research/science-for-human-rights/remote-sensing-for-human-rights.

For human rights practice – understood as fact-finding, advocacy, and litigation toward accountability, transparency, and justice – the fundamental problems with technology transfer are not limited to funding, but also include decision-making and design. Most technology is designed in places like the United States and the United Kingdom for practitioners and activists in the Global South, but generally without their involvement or input. A concerning example of this can be seen in Google’s Jigsaw project. Previously known as Google Ideas, it was re-launched in 2016 with the goal of “investing in and building technology to expand access to information for the world’s most vulnerable populations.”¹⁰ Although this project may have been created in part out of genuine and bona fide good intentions, it is in reality an example of the kind of power-consolidating technology transfer that could harm the development of a sustainable and fair human rights technology ecosystem. As the technology law and policy scholar Julia Powles argues, human development and human rights are too complex and too culturally diverse to be addressed by profit-driven companies acting on their own initiative.¹¹ More to the point, as Rikke Frank Jørgensen points out in Chapter 11, the debate on binding human rights obligations upon companies has been ongoing for more than two decades, and the private sector has continued to be largely resistant to human rights frameworks.

The effect of this type of model – in which technology is designed for, but not with, practitioners – is twofold. First, it makes it more likely that a given technological “solution” will address a false dilemma, because there is little consideration of the context in which a particular technology will be deployed, what it may be displacing, and what social or cultural practices it may be enhancing or altering. Understanding the cultural impact of technology transfer is paramount, as technology is by nature disruptive. It would be naive, and potentially detrimental to the advancement of human rights, to think that the effects can be controlled and isolated to a particular issue. Designing technology without the stakeholders at the table could also mean a lost opportunity to learn from other approaches to problem solving, thus limiting the types of solutions that can be imagined.

Second, this model can lead to investments that are unsustainable on the ground. The yearly budget for a software developer in the Global North may be equivalent, for example, to the annual budget of a small organization that provides direct support to hundreds of migrants at the border between Mexico and Guatemala. Should we create expensive technology in their name from our comfortable seats in London, New York, or Palo Alto? Or should we bring them to the table to design a sustainable solution that recognizes their agency and goals? Should we even rely on for-profit companies to tackle complex

¹⁰ E. Schmidt, “Google Ideas Becomes Jigsaw,” Jigsaw, February 16, 2016, <https://medium.com/jigsaw/google-ideas-becomes-jigsaw-bcb5bdo8c423>.

¹¹ J. Powles, “Google’s Jigsaw project has new ideas, but an old imperial mindset,” *The Guardian*, February 18, 2016, www.theguardian.com/technology/2016/feb/18/google-alphabet-jigsaw-geo-political-games-technology.

geopolitical and cultural issues of global significance? Or should we create an open and distributed ecosystem that acts in the public interest?

When we think of the future, we must keep the sustainability of the human rights movement front and center. We need to guard against technology transfer creating dependence, exporting inequalities, or promoting a paternalistic relation between technology providers and human rights practitioners. The current approach to technology is instead largely based on the model of international cooperation for development, which Shabalala shows in Chapter 3 to be deficient on many levels. While his analysis focuses on new frameworks for organizing technology transfer at the government level, I wish to focus on efforts within the human rights community itself. In human rights practice, we can create better conditions for technology to effectively advance accountability, transparency, and justice if we move away from a technocratic approach and embrace the idea of transnational solidarity. International aid, like charity, is based on an asymmetrical relationship between a party in need and another party with resources or knowledge to share.¹² Relationships of that nature are prone to creating clientelism, dependency, and unidirectional knowledge transfer. A core motivation of this chapter is to suggest a solidarity-based framework as an alternative approach to technology transfer. A first step in that direction is for practitioners to educate themselves about the technology that will be the subject of that transfer.

III WHAT IS HUMAN RIGHTS TECHNOLOGY?

Human rights practitioners frequently work in under-resourced, high-pressure environments. They tend to use opportunistic and adaptive approaches to problem solving. Because of the financial constraints that most human rights practitioners face, few technologies have been developed specifically for human rights practice. Instead, practitioners have adapted the majority of tools they use in the field from existing technologies. There are a small number of exceptions, composed largely of software projects around information management or communications. This includes projects like Martus¹³ and OpenEvsys,¹⁴ which were created specifically for human rights documentation, and privacy-enhancing mobile apps like those created by the Guardian Project. It also includes projects like PGP encryption and the Tor Internet browser, which were created by forward-thinking individuals who understood very early on in the information era that privacy and anonymity were instrumental to human rights.

Beyond these examples, the vast majority of technologies used in human rights practice are based on creative or opportunistic adaptations of general-purpose

¹² B. Prainsack and A. Buyx, "Thinking Ethical and Regulatory Frameworks in Medicine from the Perspective of Solidarity on Both Sides of the Atlantic" (2016) 37(6) *Theoretical Medicine and Bioethics* 489–501.

¹³ "Overview," Martus, <https://martus.org/overview.html>.

¹⁴ "About OpenEvsys," OpenEvsys, <http://openevsys.org/about-openevsys/>.

technologies. Today, practitioners rely on WhatsApp and Telegram to communicate with their peers or the subjects of their work; WordPress or Drupal to promote their ideas; Dropbox or Google Drive to manage their files; Google Apps or G Suite to collaborate on documents; and Skype to engage in meetings and interviews.

A significant difference between the few examples of purpose-built human rights technology and the general-purpose technology adopted and adapted by practitioners is the nature of the software behind them. Those solutions that have been created for human rights-specific purposes are largely open source. This means that the developers made the code they used to build the technology publicly available for anyone to review and tinker with. The only requirement for those who make changes or additions to open source software is that they, in turn, allow others to freely use and modify their contributions.

The foundations and donors that support the human rights movement acted as positive agents of change in promoting the use of open source software. Nearly a decade ago, they began to request that the technology created with their support be designed as open and available to others. This is key for sustainability and replication, and quite likely allows donors to maximize the impact of their portfolios. This openness, especially if expanded beyond software, will be pivotal for the inclusion of Global South and grassroots organizations in the design, adoption, and evaluation of solutions that are tailored for them. Open source software is not necessarily cheaper to develop, but it is often available with few licensing and use restrictions. It also reduces dependency and promotes collaboration among distributed and culturally diverse communities.

An important consideration when thinking about technology is the fact that the same type of adaptation that human rights practitioners can make to advance accountability, transparency, and justice could be made by other actors – from governments and corporations to organized criminals and non-state actors. In that sense, most technologies could have dual or multiple uses, including for abuse and repression of human rights. For that reason, and as Lea Shaver concludes in Chapter 2, it is critical that human rights practitioners find avenues to exercise scrutiny and oversight over technological developments in order to minimize harm.

Finally, we must consider what type of technology we should be prepared to confront in the future. What most practitioners assume fits under “human rights technology” lies within the realm of information and communication technologies, or ICTs. But the uses of technology in the human rights context already go beyond this domain. Contemporary examples of this include the use of remote sensing by international organizations to find incidents of violence¹⁵ or cultural heritage destruction,¹⁶ the growing interest in unmanned aerial vehicles (UAVs, or drones)

¹⁵ A. Marx and S. Goward, “Remote Sensing in Human Rights and International Humanitarian Law Monitoring: Concepts and Methods,” (2013) 103(1) *Geographical Review* 100–11.

¹⁶ “Case Against M. Al Mahdi,” International Criminal Court, <http://icc-mali.situplatform.com/>.

to access unreachable areas,¹⁷ and the use of DNA technology by forensic anthropologists to uncover evidence of mass atrocities.¹⁸

IV WHAT TECHNOLOGICAL TRENDS COULD SHAPE THE FUTURE OF HUMAN RIGHTS PRACTICE?

Popular culture plays an important role in shaping the way that human rights practitioners think about technology. We tend to be very generic when discussing the effects of technology in society. For example, it is common to see contemporary issues framed as “the impact of social media” on relationships or “the effect of mobile technology” on the economy, rather than on how companies, governments, communities, and individuals have integrated technology into our lives and societies. Thinking of technology as an entity divorced from human action is an inadequate starting point for discussing the future of human rights technology. If we were to follow that line of abstraction, we would risk ending up with a teleological framing of technology that authors like Kevin Kelly have proposed.¹⁹ For Kelly, there is a super-organism of technology, a “technium,” in the global interconnected system of technology that is “partly indigenous to the physics of technology itself.” To think of the future of human rights technology, we need to avoid that path. Humans have created technology, and humans have used technology to alter society. We should avoid giving agency to technology and remind ourselves constantly that technology is created by people and organizations with agendas. These are agendas that will impact us, and we should aim to influence them.

To effectively shape these agendas, practitioners need a better and more specific understanding of the trends that will shape the future of human rights technology. In digital security, for example, we can expect an expanded use of technology, including end-to-end encryption, a system of communication in which encryption ensures that only the intended recipient can read the message; multifactor authentication, a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism; and zero-knowledge encryption, a process that prevents a service provider from knowing anything about the user data that it is storing or transmitting.

In issues related to research and fact-finding, we can expect an increased use of UAVs, or drones, resulting in an increased availability of aerial images for

¹⁷ D. Whetham, “Drones to Protect,” (2015) 19(2) *The International Journal of Human Rights* 199–210.

¹⁸ M. Doretti and C. Snow, “Forensic Anthropology and Human Rights,” in D. Steadman (ed.), *Hard Evidence: Case Studies in Forensic Anthropology* (Upper Saddle River, NJ: Prentice Hall, 2003) pp. 290–310; S. Wagner, *To Know Where He Lies: DNA Technology and the Search for Srebrenica’s Missing* (Oakland: University of California Press, 2008); A. Rosenblatt, *Digging for the Disappeared* (Redwood City, CA: Stanford University Press, 2015), p. 1.

¹⁹ K. Kelly, *What Technology Wants* (New York: Penguin, 2010).

documentation of human rights and humanitarian situations²⁰; an expanded use of remote sensing and satellite imagery, which has become less expensive and more available as more firms enter the market and satellite technology improves²¹; and an increased use of open source intelligence, knowledge produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific investigative requirement.²²

In the case of advocacy, we are likely to see an expanded use of complex visualization to support the narrative of human rights accountability efforts. The work of SITU Research, an organization working in design, visualization, and spatial analysis to facilitate the analysis and presentation of evidence documenting the destruction of sites of cultural heritage in Timbuktu, Mali, is an excellent example. Created in collaboration with the International Criminal Court's Office of the Prosecutor, SITU Research built a platform that combines geospatial information, historical satellite imagery, photographs, open source videos, and other forms of site documentation. The Office of the Prosecutor used SITU's tool successfully at the trial proceedings at the International Criminal Court in 2016.²³ This work is part an emergent field called forensic architecture, first developed at Goldsmiths College, University of London.²⁴ It refers to "the practice of treating common elements of our built environment as entry points through which to interrogate the present."²⁵

The continued development of areas and projects like these will also be accompanied by new efforts in areas where technological trends are moving rapidly. While not exclusive, concepts like artificial intelligence, blockchain, sensors, open source hardware, and the Internet of Things reflect areas that are likely to offer fertile ground for the development of human rights technology and applications.

A Artificial Intelligence

Perhaps nothing embodies our fascination with and fear of technology better than artificial intelligence (AI). There are countless images in popular culture that

²⁰ K. Kakaes et al., *Drones and Aerial Observation: New Technologies for Property Rights, Human Rights, and Global Development: A Primer* (Washington, DC: New America, 2015).

²¹ J. Kumagai, "9 Earth-Imaging Start-Ups to Watch," *IEEE Spectrum*, March 28, 2014, <http://spectrum.ieee.org/aerospace/satellites/9-earthimaging-startups-to-watch>.

²² E. Higgins, "A New Age of Open Source Investigation: International Examples," in B. Akhgar et al. (eds.), *Open Source Intelligence Investigation* (New York: Springer International Publishing, 2016) pp. 189–196.

²³ See Kelly, *What Technology Wants*.

²⁴ E. Weizman, "Forensic Architecture: Violence at the Threshold of Detectability" (2015) 54(4) *E-flux Journal* 1–17.

²⁵ Y. Bois et al., "On Forensic Architecture: A Conversation with Eyal Weizman" (2016) 156 *October* 115–40.

evidence this, and while the reality is different than the anthropomorphic version of what we see on the big screen, AI is no less fascinating in reality.

AI is premised on the notion that “every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it.”²⁶ Scientists have been working to make this dream a reality for several decades, but a critical milestone, the equivalent of the “man-on-the-moon moment,” happened in late 2015 when AlphaGo, a computer program developed by Deep Mind, a UK company recently acquired by Google, was able to defeat the best human player in the world at the ancient game of Go.²⁷ The game of Go, which was invented in China thousands of years ago, has a number of possible legal moves larger than the number of atoms in the observable universe. It is this complexity that made it a sizable test for artificial intelligence.

Generally speaking, AI is divided into weak AI and strong AI. Most artificial intelligence applications so far are considered either an expert system (ES) or a knowledge-based system (KBS), which means that they rely on an existing model or corpus of knowledge. This is, in a way, the application of existing knowledge to assess the best answer to a question or problem. This form of AI is generally referred to as “weak AI” because it requires *a priori* knowledge to arrive at the answer to a question. “Strong AI,” on the other hand, generally refers to the ability of a machine to perform “general intelligent action,” which is why it is also referred to as artificial general intelligence. In the case of the AlphaGo scenario, this meant that instead of evaluating all possible moves to calculate all possible outcomes like an ES or KBS would do, AlphaGo thought and made decisions like a human. The extraordinary achievement of AlphaGo is that it is not an expert system, but rather relies on artificial general intelligence. In other words, it *learned* to play Go rather than being fed many possibilities and choosing the one that best fit a particular scenario. This is generally accepted as evidence that AI has reached a tipping point much sooner than most scientists thought it would.

How can all this be of use for human rights practice? Can a machine teach itself to solve human rights problems? Will this be an opportunity or a challenge for human rights practice? In thinking of the future, I would argue that it is more likely that human rights practice will first benefit from advances in specific areas of AI research like machine learning, computer vision, and natural language processing, not in automated decision-making. These advances will improve the ability of human rights researchers to discover, translate, and analyze relevant information.

To get a sense of what may be possible, we can look at some recent experimental uses of AI for human rights issues. Researchers at the University of Sheffield and the

²⁶ John McCarthy et al. “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955” (2006) 27(4) *AI Magazine* 12.

²⁷ C. Moyer, “How Google’s AlphaGo Beat a Go World Champion,” *The Atlantic*, March 28, 2016.

University of Pennsylvania have used AI to develop a method for accurately predicting the results of judicial decisions of the European Court of Human Rights. The research team identified 584 cases relating to three articles of the European Convention on Human Rights: Article 3, concerning torture and inhuman and degrading treatment; Article 6, which protects the right to a fair trial; and Article 8, on the right to respect for a private and family life. After running their machine learning algorithm against this dataset to find patterns in the text, the team was able to predict the verdicts at an accuracy of 79 percent. What this suggests is that AI could be used to build predictive models to discover patterns in judicial decisions. This approach could help increase the success and effectiveness of litigation in defense of human rights by assisting advocates and lawyers in planning their litigation strategy.

Another example of the potential use of AI to advance human rights practice can be found in the work of the Center for Human Rights Science (CHRS) at Carnegie Mellon University.²⁸ After hearing of the challenges that human rights organizations were facing in analyzing and verifying the large volume of online videos regarding human rights abuses, researchers at the CHRS began to experiment with AI applications to solve these problems. With the goal of creating efficient and manageable workflows for human rights practitioners, they have created computer vision and machine learning methods to rapidly process and analyze large amounts of video. Their tools help human rights practitioners detect audio like explosions, gunshots, or screaming in video collections; detect and count the number of people in a given frame of a video; aid in geolocation of a video; and synchronize multiple videos taken by different sources at the same time and place to create a composite view of an incident.

But perhaps the most sophisticated use of AI applied to human rights that we can find is in the center's Event Labeling through Analytic Media Processing (E-LAMP) system.²⁹ E-LAMP is a machine learning and computer vision-based video analysis system that is able to detect objects, sounds, speech, text, and event types (say, a news broadcast or a protest) in a video collection. In practice, this allows users to run semantic queries within video collections. If the system is properly trained, a user could ask it, for example, to find images of individuals performing a specific action or objects of a particular kind in a collection of thousands of videos. This means that practitioners can use a system that can search thousands or even millions of videos to answer questions like: How many videos show helicopters dropping things (e.g., barrel bombs or bodies)? How many videos may be communiques from a faction within a conflict? What are the commonalities among a group of videos? These search efforts can be done in a fraction of the time that it would take for a human

²⁸ The author is program manager and co-founder of the Technology Program at the Center for Human Rights Science, Carnegie Mellon University.

²⁹ Jay D. Aronson, Shicheng Xu, and Alex Hauptmann, "Video analytics for conflict monitoring and human rights documentation" (2015).

analyst to perform the same task. AI projects like E-LAMP will make practitioners more effective by allowing small teams to quickly examine and analyze large amounts of evidence. While systems like this could become valuable automated research assistants that aid in the process of knowledge discovery, they will remain instruments for human domain experts. E-LAMP cannot yet find all actions that are relevant for a case, for example, torture or physical abuse, but it is able to find potential markers for those actions that could then be reviewed by a practitioner.

The big opportunity for human rights practice lies in the extraordinary potential that artificial intelligence has to support problem solving, pattern detection, and knowledge discovery. But this kind of capability will not simply materialize from thin air. There is a time-bound opportunity for practitioners to influence artificial intelligence before it completely leaves its infancy. Legal experts could provide important guidance as to how, ethically, AI's findings could be verified in courts, how AI may shape the definition of legal personhood, and how data being analyzed in the cloud can be protected from exposure to nefarious actors. For this, human rights practitioners need to engage early and often with the technologists and organizations that are driving the technological future of AI.

B Blockchain

In 2008, a person or group of persons under the pseudonym Satoshi Nakamoto published a paper proposing Bitcoin, a peer-to-peer electronic currency aimed at supporting transactions without a central financial institution.³⁰ Since then, Bitcoin has drawn attention from a wide variety of actors and entities, ranging from banks and regulators to organized criminals and futurists. Looking back, it is not hard to see why it is considered a potential disrupter of national, regional, and international financial systems. It took only two years from its formal launch in 2009 for this revolutionary virtual currency to achieve parity with the US dollar.³¹ And it took only a few additional years to reach an all-time-high \$1,216.73 exchange rate.³² Surprisingly, all of this happened with a decentralized, public, and open infrastructure.

But beyond its disruptive capacity and its direct challenge to institutions that reproduce and maintain inequalities, like banks and international financial regulators, there are other aspects of Bitcoin that could advance the future of transparency and accountability. Its potentially transformative power for human rights practice is anchored in the innovative design of the technology underneath the currency that facilitates public trust without the need for a third party controlling the currency. This technology is commonly referred to as “blockchain.”

³⁰ S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” <https://bitcoin.org/bitcoin.pdf>.

³¹ L. Literak, “Bitcoin dosáhl parity s dolarem,” *AbcLinuxu*, February 22, 2014, www.abclinuxu.cz/zpravicky/bitcoin-dosahl-parity-s-dolarem.

³² “History of bitcoin,” *Wikipedia*, https://en.wikipedia.org/wiki/History_of_bitcoin.

Blockchain refers to a distributed network of computers in which digital transactions are recorded in a public database using cryptography to digitally sign them and connect them to previous transactions. This process creates a chain of grouped transactions, or blocks, that cannot be tampered with or altered. One way to think of this is as if everyone in a network of peers acted as a digital notary. In this network, transactions are notarized by multiple notaries, and notaries publicly broadcast the existence of a record by linking it to an existing and already notarized transaction or document in a public ledger. Among the most interesting attributes of such a system is the fact that trust is not placed in the nodes, but rather in the strength and openness of the network and the science behind the protocol for transactions.

Outside of currency exchange, people can access bitcoins not by labor, but rather by computation. The currency is ephemeral and is not backed by gold or any other representation in the physical space. Its creation is the result of software and hardware computations that have to solve increasingly complex mathematical operations. Once a solution is found, bitcoins are the reward. This process is called “mining.” Each one is awarded to the person behind the computation using a unique identifier, also the result of computation, that the user obtains when installing the mining software. Such a key is also referred as a wallet, and the wallet is where the awarded (or purchased) bitcoins are stored. In other words, besides exchanging them directly, as a person could do with any foreign currency, the only way to get them is by solving computational problems.

Blockchain has several human rights applications. It could be used to certify that a video, image, or other type of digital document existed at a given time. This attribute, normally referred as proof of existence, increases the evidentiary weight of a digital asset, like a video or image of human rights abuse that appeared in social media, by increasing the ability of investigators to validate or reject claims of authenticity over the material and map its chain of custody. Preliminary uses of this technology can be seen in projects like Video Vault,³³ a system that I created and maintain, which allows human rights practitioners to preserve digital resources of any kind for later reference. Video Vault facilitates the verification of digital assets by providing an online content sample with a trusted time stamp³⁴ reflecting the collection time. This time stamp is added as a transaction to the blockchain, where it can be accessed to validate that such asset, picture, video, or web page existed at a particular point in time. Digital assets collected by an individual or organization can in this way be “notarized” and added to the blockchain to create a public ledger, to enhance the verification of media that may contain evidence of human rights abuses.

It is also possible to imagine applications for blockchain technology in other areas of social activity that relate to human rights practice. One example is trade and the

³³ Video Vault, www.bravenewtech.org/.

³⁴ A trusted time stamp is a form of proof of existence that relies on a trusted third party to create and maintain a hash of a file to certify that a particular asset existed at a given time. A hash is a unique alphanumeric string created from the digital file that is time-stamped using cryptography and allows tracking of the creation and modification of a file.

distributed manufacturing or production of goods. Technology like blockchain could be used to create a chain of trust or custody around specific steps of manufacturing, thus increasing the ability to monitor the life cycles of the goods we consume. Such a system could, at least in theory, enhance the ability of agencies, unions, regulators, and civil society to enforce compliance with laws and guidelines that defend the rights of workers, indigenous people, and the environment, to name a few.

This traceability feature is already part of the offerings of companies like Provenance³⁵ to food producers and supply chain watchdogs. What is learned from this process could benefit its implementation in fact-finding in human rights practice. Provenance is a UK-based company using currencies like Bitcoin and Ethereum, which are implementations of blockchain, to create a public record of the supply chain from the origin of a product to its end consumer. This technology could help consumers learn where their clothes were made or where the fish they are thinking about purchasing for dinner was netted. Perhaps more importantly, it could help consumers understand the environmental and labor conditions where their goods were produced or obtained.

As is often the case with new technologies, a group of forward-looking technologists and entrepreneurs have proposed other creative applications for blockchain, including to increase transparency and reduce corruption in public spending by governments or the use of charitable funds; to create efficient ways to transfer currency to support basic rights, like access to health care and food security, when traditional financial institutions fail in the context of humanitarian crisis; to create alternative and inclusive systems for land registration for migrants; or to provide access to identities in order to prevent discrimination of ex-convicts.

A recently formed e-governance consultancy called Humanitarian Blockchain³⁶ is attempting to make some of these ideas a reality. Because of its distributed and open nature as well as its reliance on sound mathematical concepts, blockchain is resistant to manipulation. It does not matter if a large government or a local paramilitary organization disagrees with what it carries. Because of its distributed nature, the public ledger will remain unmodified and available to its users. Recently, researchers from the Massachusetts Institute of Technology and Tel Aviv University proposed a decentralized personal data-management system that would ensure that users own and control their data. Such a system would enhance the privacy of sensitive data, including that of human rights practitioners.³⁷

Today, blockchain-based systems may be complicated to access and understand by grassroots organizations, but this will rapidly change. It is likely that at this pace,

³⁵ T. Levitt, "Blockchain technology trialed to tackle slavery in the fishing industry," *The Guardian*, September 7, 2016, www.theguardian.com/sustainable-business/2016/sep/07/block-chain-fish-slavery-free-seafood-sustainable-technology.

³⁶ Humanitarian Blockchain, Facebook, www.facebook.com/HumanitarianBlockchain.

³⁷ G. Zyskind and O. Nathan, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops (SPW)*, Washington, DC, May 21–22, 2015, pp. 180–84.

just as it is beginning to happen with encryption and security mechanisms like Secure Sockets Layer/Transport Layer Security (SSL/TLS), which is used to secure most transactions over the Internet, and end-to-end encryption, which is used to secure communications on tools like WhatsApp and Signal, the benefits of this technology will soon be available in seamless, low-cost ways for practitioners of all kinds.

C Open Hardware, Affordable Sensors, and the Internet of Things

For many years, human rights technology has been limited to software. Software can be written on virtually any computer. There are also numerous well-documented programming languages that, with some patience and basic literacy, anyone can learn. Furthermore, there is no need for a project to start from scratch, because with the growth of open source and free software, many libraries and code bases can help anyone jump-start a project. Such availability and simplicity were, without a doubt, key to the explosion of software products for many disciplines, including human rights practice.

Over the past decade, slowly but incrementally, hardware has followed suit. Similarly to software, the advent of open source hardware has created a vast arena for experimentation and has expanded the toolkit for problem solving that practitioners can access. In 2003, Hernando Barragán, a master's student at the Interaction Design Institute Ivrea in Italy, created Wiring as part of his thesis project. Wiring was aimed at lowering the barrier to accessing prototyping tools for those interested in developing electronics. It consists of the complete tool set needed to develop functional electronic prototypes, from an integrated development environment (IDE) and a simple programming language for microcontrollers to a bootloader to update programs and a well-documented online documentation library. In a controversial move, Barragán's thesis advisors and fellow students copied the project to create Arduino in 2005. Arduino rapidly became the platform of choice for a new generation of open source hardware tinkerers. By 2013, there were 700,000 Arduino devices registered and at least an equal number of clones or copies. The number of prototyping platforms grew, and there are now dozens of different boards and platforms to choose from. The projects enabled by this new generation of hardware range from simple LED controlling projects to sophisticated motor control and sensor management devices. Some of these projects illustrate what we could see at the intersection of human rights practice and open hardware in the near future, especially as issues of environmental justice are increasingly rooted in human rights, including but not limited to nuclear disasters, oil spills, and water safety.

An important example of environmental justice-oriented open hardware involved the creation of sensors to measure radioactivity in the aftermath of the March 11, 2011 earthquake and destructive tsunami that severely damaged the Daiichi nuclear power plant in Fukushima, Japan. The radiation leak that occurred at the power

plant was followed by panic and misinformation. Citizens with enough money acquired Geiger counters to measure the scale of the catastrophe, both for personal safety and for the eventual accountability of officials whom they felt were not appropriately responding to the crisis. These devices, which are designed to measure ionizing radiation, became a critical source of reliable information for the affected population. During the early response, the supply of these devices began to decline and prices became too high for many citizens to purchase them. A group of developers, activists, and responders held Skype discussions to brainstorm a possible solution. After a few days, this group met in person at Tokyo Hackerspace. Within a week, they had created the first bGeigie, a DIY Geiger counter that could increase access to reliable data, and they set off for Fukushima. Today, that project has evolved into Safecast, founded by Sean Bonner, Joi Ito, and Pieter Franken as an international, volunteer-centered organization devoted to open citizen science for the environment.³⁸ A similar story is that of the Public Laboratory for Open Technology, founded in the wake of the April 2010 Deepwater Horizon oil spill in the Gulf of Mexico on the BP-operated Macondo Prospect. During the spill, there was an information blackout for residents of the region. In response, a group of concerned residents, environmental advocates, designers, and social scientists launched DIY kite and balloon aerial photography kits over the spill to collect real-time data about its impact.³⁹ The success of the mapping effort encouraged the group to found Public Lab as a research and social space for the development of low-cost tools for community-based environmental monitoring and assessment. Among the tools that Public Lab offers is a Desktop Spectrometry Kit, which puts a low-cost, easy-to-use spectroscope or spectrophotometer in the hands of any individual or organization interested in collecting spectra, which are the electromagnetic “fingerprints,” or unique identifiers, of materials.⁴⁰

The above examples comprise a small sample of the vibrant community around microcontrollers, sensors, and citizen science. They can help us imagine how the availability of easy-to-use and low-cost sensors and measurement kits may have a transformative effect in the future of human rights. Could we measure the fingerprint of a tear gas canister with sufficient accuracy to point to its origin? Could we allow for communities to directly and reliably collect information about the quality of the water before and after an extractive industry development? Could we take samples with remote equipment of chemical agents used against vulnerable populations? Human rights practitioners need to engage with the vibrant open source hardware community to find answers to questions like this. While the above uses

³⁸ M. Prosser, “How a Crowd Science Geiger Counter Cast Light on The Fukushima Radioactive Fallout Mystery,” *Forbes*, March 10, 2016, www.forbes.com/sites/prossermarc/2016/03/10/how-a-crowd-science-geiger-counter-cast-light-on-the-fukushima-radioactive-fallout-mystery/.

³⁹ Public Lab contributors, “Public Lab: Gulf Coast,” <https://publiclab.org/wiki/gulf-coast>.

⁴⁰ Public Lab contributors, “Public Lab: Desktop Spectrometry Kit,” <https://publiclab.org/wiki/dsk>.

may not yet seem related to traditional human rights work, this may change rapidly as environmental issues, like those related to extractive industries or access to water, permeate human rights practice. More importantly, technologies like those discussed above are aligned with the type of technology transfer that Dalindyebo Shabalala calls for in Chapter 3, both because they enable low-cost and broad access, and because they can contribute to the creation of complex monitoring ecosystems that could inform future human rights frameworks.

Hardware is not only sensors and microcontrollers. Over the past ten years, there have been efforts to reduce the cost of, and increase access to, computers. Perhaps the most known example of this is Raspberry Pi. Raspberry Pi is a series of credit card-sized single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and developing countries.⁴¹ More importantly, it is open source and available anywhere in the world for under \$50. The advent of this device has created a great deal of excitement among developers and technologists, as the processing power and the possibilities are immense when compared to a microcontroller like Arduino. This excitement can be seen in its adoption. Since the launch of its first model, the Raspberry Pi 1 Model B, in February 2012, more than ten million have been sold.⁴² Enthusiasts and developers have started to create potentially relevant projects for human rights practice. For example, developers have used Raspberry Pi computers to create specialized routers that increase the anonymity of their users. Others have created advanced remote sensor units that can automatically consume data and broadcast it in real time.

The Novena laptop, launched in 2014, was designed for users who care about free software and open source, or who want to modify and extend their hardware. Its creator, Andrew “bunnie” Huang, promoted it as “a laptop with no secrets.”⁴³ It is this claim that makes the Novena interesting for the future of human rights practice. A laptop with nothing but modifiable and open source hardware and software may allow practitioners to access hardware that they can trust to carry out sensitive work and transfer sensitive information. Open source hardware and software are potentially more trustworthy than proprietary technology, as they can be reviewed and audited by anyone who is willing to do so.

The future of Novena is unclear, as it has not yet found commercial success, but its existence has ignited a generation of entrepreneurs willing to compete with large manufacturers to offer options for general users. An important example

⁴¹ Raspberry Pi Foundation, “About Us,” www.raspberrypi.org/about/.

⁴² “Sales Soar and Raspberry Pi British Board Beats Commodore 64,” *The MagPi Magazine*, March 16, 2017, www.raspberrypi.org/magpi/raspberrypi-sales/.

⁴³ A. Huang and S. Cross, “Novena: A Laptop With No Secrets,” *IEEE Spectrum*, October 27, 2015, <http://spectrum.ieee.org/consumer-electronics/portable-devices/novena-a-laptop-with-no-secrets>.

of this is the Librem 13, a laptop available since 2016 that promises to respect privacy and enhance security in “every chip in the hardware, every line of code in the software.”⁴⁴ The laptop ships with the option of two operating systems, Purism OS or Qubes OS, which are both well regarded in the security and open source communities as strong and reliable options for those with security and privacy in mind. It also includes hardware kill switches that shut down the microphone, camera, Wi-Fi connection, and Bluetooth. These are important characteristics that practitioners should consider, given the scope of unchecked surveillance by governments exposed to a broad public by the revelations of Edward Snowden and other whistleblowers, as described by Lisl Brunner in Chapter 10.

If these devices survive and evolve, or if they encourage other open and secure products, they will provide valuable tools for human rights practitioners seeking to protect the data of vulnerable populations. As the market for open source or privacy-enhancing hardware is in its early stages of development, it is unclear whether the scale of production will be sufficient to reach human rights practitioners around the globe. Scale will not only impact the affordability of a device, but also determine whether it moves into common usage. If it does not, it could raise red flags for governments when crossing borders or adversarial checkpoints.

It is essential that secure tools are not just available for human rights researchers but are also adopted by wider communities. The general adoption of features by nonspecialized products makes the use of these features by human rights researchers less risky, because they are less identified with behavior the state wants to control. A powerful example of this is the adoption of end-to-end encryption by the popular messaging application WhatsApp. In 2016, WhatsApp announced that it was making end-to-end encryption the communication default for its billion-plus users.⁴⁵ The notion of end-to-end encryption, which refers to the use of communications systems in which only the originator and recipient of a message can read its contents, is nothing new to human rights practice. For many years, dozens of human rights and technology advocates have promoted end-to-end encryption as critical for the future of journalistic and human rights work,⁴⁶ but it was not until this development that such technology became widely available. If projects like the Novena and Librem 13 laptops successfully compete for a small fraction of the market share of companies like Lenovo and Hewlett-Packard, they could create pressure for other manufacturers to adopt the privacy-enhancing features that distinguish them, and in doing so offer secure computing alternatives for human rights practitioners.

⁴⁴ Purism, “Discover the Librem 13,” <https://puri.sm/products/librem-13/>.

⁴⁵ “End-to-End Encryption,” *WhatsApp Blog*, April 5, 2016, <https://blog.whatsapp.com/10000618/end-to-end-encryption>.

⁴⁶ Access Now, “Encryption TK: Securing the Future of Journalism and Human Rights,” YouTube, March 20, 2014, www.youtube.com/watch?v=uxidkrhOo-o.

Beyond the expansion of these existing technologies, we are also likely to see innovation around the Internet of Things, or IoT, which references the increased connectivity or networking among devices of all kinds and purposes. The IoT, which allows the devices of smart homes and smart cities to be controlled remotely, and in many cases automatically, is linked directly to the growing availability of open hardware and sensors. From thermostats and refrigerators to wearable devices and new forms of personal and mobile devices, we are likely to see connected devices in virtually every aspect of human life. This will likely create excellent opportunities for new forms of fact-finding and research, but will also likely create new perils for human rights practitioners and general users alike. Perhaps the biggest challenge will come from the ability that governments and organized criminals have developed to access and analyze data stored and in transit. We are only starting to understand what this might mean, for instance in recent analyses of the privacy implications of fitness trackers,⁴⁷ for how law enforcement could use our intelligent personal digital assistants in criminal and national security investigations,⁴⁸ and how connected home cameras could be infiltrated by organized criminals, governments, and other nefarious actors.⁴⁹

V CONCLUSION

Events of the past five years have significantly shaped the discourse around human rights technology. What has been learned and confirmed after Edward Snowden's revelations of mass and unchecked surveillance by nation-states and corporations has necessarily focused the attention of global civil society on the dire effects of surveillance and the need to counter them.⁵⁰ The state of surveillance has cast a dystopian shadow over the future of human rights, as Mark Latonero points out in Chapter 7, where practitioners fear technology will be used for control rather than liberation. The hypersurveillance practices of our times, as well as the role that technology plays in them, are indeed an extensive attack on human rights.⁵¹

⁴⁷ A. Hiltz, C. Parsons, and J. Knockel, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," *Open Effect* (2016).

⁴⁸ A. Wang, "Can Alexa help solve a murder? Police think so – but Amazon won't give up her data," *The Washington Post*, December 28, 2016, www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/.

⁴⁹ "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," *Krebs on Security*, October 21, 2016, <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>.

⁵⁰ E. MacAskill et al., "NSA Files: Decoded: What the revelations mean for you," *The Guardian*, November 1, 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

⁵¹ E. Piracés, "From Paranoia to Solidarity: Human Rights Technology in the Age of Hyper-Surveillance," Canada Centre for Global Security Studies, March 28, 2014, www.cyberdialogue.ca/2014/03/from-paranoia-to-solidarity-human-rights-technology-in-the-age-of-hyper-surveillance-by-enrique-piraces/.

However, human rights practitioners should not let that hinder their ability to imagine alternative visions that could guide the intersection of human rights and technology.

The technologies discussed in this chapter do not represent an exhaustive compilation of trends that will shape the future of human rights practice, but rather are a starting point to expand our understanding of what technology could do for us in the near future. Challenging current technology transfer models and expanding the ecosystem of actors around them is key, because in creating a more inclusive, deliberate, and forward-looking interdisciplinary field around human rights technology, we will be creating a better opportunity to advance the larger human rights field.

A change in the dynamics of technology transfer will challenge the traditionally asymmetrical power dynamics between human rights practitioners and their transnational supporters. We can foster this by promoting capacity-building in the Global South, favoring open source software and hardware, and critically evaluating budgetary allotments to technology. In the process, grassroots practitioners will be at the helm of designing and adapting human rights technology. We must be conscious that this will challenge the growth of professional opportunities for Global North practitioners. There are important questions that will be critical for any next step. Can human rights play a role in the governing of technology? What role can the private sector play in advancing human rights technology? Can human rights challenges drive technological innovation? To answer them, we should be open to interdisciplinary conversations like the one taking place in this volume, and encourage an inclusive and participatory multistakeholder ecosystem.

The approach of human rights practitioners to technology will be a determining factor in their ability to advance accountability, transparency, and justice in the years to come. This book is an invitation to imagine the future of the intersection of human rights technology and human rights practice. For this intersection to benefit practitioners, it must adopt a solidarity-based framework for technology transfer.

A solidarity approach requires technologists to understand and respect the cultural context of the environment they are working within. They must reimagine the relationship as bidirectional and characterize their counterparts in technology transfer as active collaborators. Technologists must establish partner relationships with practitioners, from designing solutions that involve technology all the way through to evaluating them. Practitioners should also be able to tinker with and modify the technologies they are using, and technologists should support them in doing so. This commitment should be reflected in the timeline, budget, and conceptualization of the project. Solidarity requires careful consideration of how technology may displace human resources or compete with scarce resources available in the human rights funding landscape. This technology transfer approach

prioritizes human capacity and sustainability above technical complexity and sophistication. Finally, technologists must continuously question their own role within larger power structures – are they helping to reduce the burden of inequality and dependency, or are they just recreating it through the deployment of technology? Ultimately, a solidarity approach demands that technologists not contribute to long-term inequalities while working with human rights workers and communities in crisis.