

**April 2020**

## Human Rights and Digital Technologies: Proceedings of a Symposium of Scholars and Practitioners - in Brief

**D**igital technologies provide a means of anticipating, analyzing, and responding to human rights concerns, but they also present human rights challenges. These technologies have expanded opportunities for individuals and organizations to mobilize, document, and advocate, including around human rights and humanitarian crises; however, with these opportunities come certain concerns. Digital technologies have, for instance, been used to spread disinformation, surveil human rights defenders, and promote and incite violence. Discrimination in the use of, and access to, digital technologies presents another serious concern.

On **September 18, 2019**, the Committee on Human Rights of the U.S. National Academies of Sciences, Engineering, and Medicine (the National Academies) gathered experts in the fields of human rights and digital technology to examine these and other challenges and to explore ways of leveraging digital innovations in a manner that helps protect internationally recognized human rights. During the symposium, participants discussed the risks of both exclusion and inclusion when it comes to digital technologies, and several drew attention to the power imbalance between civil society and government/corporate actors in the digital space. Many participants emphasized the critical role of international human rights law in helping to address concerns related to digital technologies and the need for a rights-based approach to the design, governance, and use of such technologies. Although experts at the Committee on Human Rights event were primarily drawn from academia, policy institutions, and international organizations, several participants at the event pointed to the importance of engaging digital technology companies in this effort and the need for greater attention to the voices and perspectives of individuals affected by digital technologies, including marginalized populations that may face particular risks.

Numerous participants suggested that, in order to implement international human rights law effectively in

this context, human rights education is essential, together with cross-disciplinary, multi-stakeholder efforts to address rights-related challenges, such as discrimination related to artificial intelligence systems and the targeted digital surveillance of journalists, activists, and human rights defenders.

The symposium began with a keynote address, followed by a series of panels. A summary of the discussion is below.

**Martin Chalfie, University Professor, Columbia University and Chair, Committee on Human Rights, U.S. National Academies of Sciences, Engineering, and Medicine**, welcomed symposium participants and described the work of the Committee on Human Rights, which serves as a bridge between the human rights and scientific, engineering, and medical communities. The purpose of the symposium, **Chalfie** stated, was to gather experts to discuss key human rights opportunities and risks related to the rapid expansion of digital technologies.

## THE RELEVANCE OF HUMAN RIGHTS IN A DIGITAL WORLD

**David Kaye, United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression**, provided a keynote address, introducing the session by stating that Americans do not “speak human rights”; human rights are not part of the vernacular or an area of focus within the U.S. educational system, where discussion of rights tends to focus on the U.S. Constitution. International human rights law provides a common, widely agreed upon standard for addressing rights abuses occurring throughout the world. The United States is a party to some international human rights treaties, including the International Covenant on Civil and Political Rights (ICCPR). However, it has not ratified other important treaties such as the International Covenant on Economic, Social and Cultural Rights, which sets out, for instance, the human right “(t)o enjoy the benefits of scientific progress and its applications”. According to **Kaye**, lack of attention to international human rights within the United States has bred inaction. As a matter of urgency, it is important to educate and engage individuals in the United States and other individuals around the world on the international human rights framework, which includes treaties on a wide range of human rights topics, as well as mechanisms to ensure implementation of the rights contained in those



**Figure 1** David Kaye, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Source: Cable Risdon/Risdon Photography

treaties.

Human rights law — its vocabulary, framework, and vision — provides a basis for restraining the worst intrusions and violations of the digital world and promoting its best, **Kaye** said. However, he explained that much work needs to be done to move forward a human rights-oriented digital agenda that will capitalize on the benefits of digital technologies to advance human rights, while ensuring that these same technologies do not infringe on rights.

Certain foundational international human rights standards are set out in the International Covenant on Civil and Political Rights (ICCPR), a multilateral treaty adopted by the UN General Assembly which has been ratified by the United States. Article 19 of the ICCPR is a robust statement of rights that is well-suited for the digital age, said **Kaye** (see BOX 1).

**Kaye** explained that holding States accountable for human rights abuses associated with digital technologies is critical. However, he also stressed that companies should exercise human rights due diligence. Digital technology companies have become governors of online space and, in turn, are shaping freedom of expression around the world. [The United Nations Guiding Principles on Business and Human Rights](#), a framework for addressing human rights abuses in business operations, can be used to help ensure that companies respect rights. According to **Kaye**, the UN Human Rights Council’s position that “offline rights apply equally online” needs to be made a reality. If pushed, technology companies might become leaders in thinking about how human rights can have an impact on our lives and in shaping the way we think about privacy, freedom of expression, and other rights. **Kaye** referenced a recent announcement by Facebook that the company would look to international human rights standards in making judgments about expression on the platform.

**Kaye** closed by stating that holding a symposium on this topic at the National Academies was critical as a

**BOX 1. Article 19 of International Covenant on Civil and Political Rights (ICCPR)**

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
  - (a) For respect of the rights or reputations of others;
  - (b) For the protection of national security or of public order (ordre public), or of public health or morals.

way of advocating for education on human rights.

## TOWARD A RIGHTS-BASED APPROACH TO DIGITAL DATA COLLECTION AND ANALYSIS BY CIVIL SOCIETY

**Nathaniel Raymond (Panel Moderator), Lecturer, Jackson Institute of Global Affairs, Yale University,** provided a historical and theoretical perspective on issues related to data collection and human rights, describing sources of rights for subjects of data collection. He described the foundation for the current robust set of protections for personally identifiable information (PII), but stressed that we have entered an age of a new type of data, demographically identifiable information (DII). These data are the basis for algorithmic systems. The pathways to harm and human rights violations from information communication technologies and in-group data are not addressed by traditional PII-based governance. Of particular



**Figure 2** Dani Poole, Harvard University; Jos Berens, UN Office for the Coordination of Humanitarian Affairs; Jessie Brunner, Stanford University; Nathaniel Raymond, Yale University

Source: Cable Risdon/Risdon Photography

concern are digital disparities. **Raymond** stressed that having norms will not be enough without governance and accountability in the field.

**Jessie Brunner, Senior Program Manager, Center for Human Rights and International Justice, Stanford University,** introduced her research on human trafficking in Southeast Asia, which involves the use of advances in data science to better understand—and help address—this problem. **Brunner** noted that data on human trafficking have historically been focused on the prevalence of the problem.

To get a better understanding about what has been happening at the front lines, she has worked with local anti-trafficking organizations on using digital data/technology to enhance their operations. While better access to and use of technologies and digital data can help empower these organizations in meeting their objectives, many lack the technical systems and normative frameworks, as well as technical staff, to fully benefit from them. **Brunner** also stressed that ensuring data privacy and security sometimes presents a challenge.

To help address some of these issues, **Brunner** added that she has developed [guidelines](#) for digital data collection, sharing, and use for anti-trafficking practitioners in Southeast Asia. She noted that groups have been created at the local level to discuss implementation of the guidelines. Listening to the voices and

perspectives of those directly affected by data systems is critical, **Brunner** stressed.

**Jos Berens, Data Policy Officer, United Nations Office for the Coordination of Humanitarian Affairs (OCHA)**, outlined various problems related to data in humanitarian crisis settings. For instance, he discussed data hygiene and informal data-sharing, and how urgency and volatility in such settings create and compound risk. Another problem is the failure of actors providing humanitarian assistance to share information with one another, in many cases due to the lack of clear guidance on how this data should be managed. **Berens** discussed efforts by OCHA's Center for Humanitarian Data to develop a [set of data responsibility guidelines](#), a working draft of which was released in March 2019. These guidelines are an example of how existing regulation, including human rights standards, can be translated into practical guidance for the use of digital technologies. The guidelines promote 'data responsibility': the safe, ethical, and effective management of data by OCHA staff in the context of humanitarian response. The guidelines facilitate the protection of human rights, such as the right to privacy, and actively call for the sharing and use of data where appropriate. The guidelines primarily focus on non-personal but still potentially sensitive data, and the distinct set potential 'group harms' associated with the management of such data. **Berens** added that OCHA's Center for Humanitarian Data is working to test the draft guidelines, including a template information-sharing protocol (found at page 55 of the [draft guidelines](#)), in various countries, including Sudan and Yemen.

International and non-governmental organizations are not generally at the forefront of technological development, **Berens** stated, but they can play a role in helping to develop value-sensitive and rights-based technologies as well as in the development of governance for such technologies.

**Dani Poole, Postdoctoral Fellow, Harvard Humanitarian Initiative, Harvard University**, described her work as population health science, examining the intersection between technology and human rights during humanitarian crises. The importance of having a mobile phone during a crisis cannot be stressed enough, **Poole** noted; it provides a platform for realizing the right to health (e.g., as a means of finding health facilities, helping to alleviate anxiety about loved ones).

**Poole** raised questions about what informed consent for data collection should look like in the context of humanitarian crises. She described the [General Data Protection Regulation \(GDPR\)](#) as being positive in terms of consumer privacy protection but observed that it can be challenging to implement in certain research settings.

**Poole** also emphasized the need to pay attention to whose voices are included in data collection initiatives and noted that those of women and children are often excluded in humanitarian settings (due, for instance, to a reliance on the head of household for information). It is also important to explore how technology is

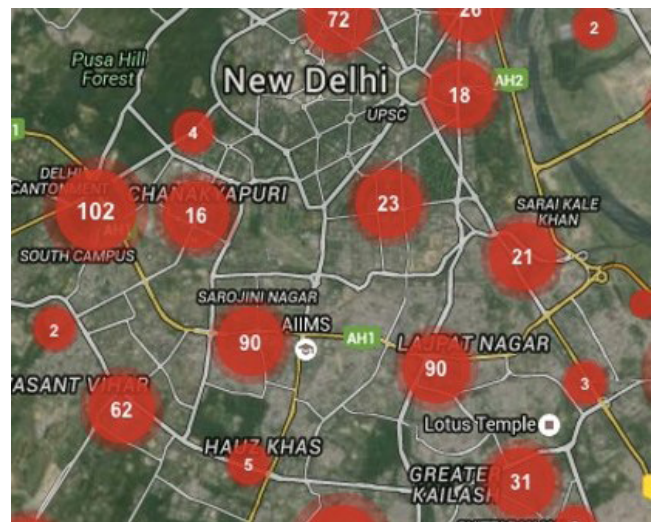
used in humanitarian settings. As an example of the gender digital divide, women are less likely to own a mobile phone than their male peers.

## PROMOTING ACCOUNTABILITY AND JUSTICE WITH DIGITAL DATA

**Tanya Karanasios (Panel Moderator), Deputy Program Director, WITNESS**, outlined her work with a non-governmental organization addressing issues at the intersection of human rights, technology, and video, pointing to the proliferation of cell phones and its significance for human rights advocates seeking to document and report on potential human rights violations. For example, **Karanasios** discussed how members of the Afro-Brazilian community were able to raise greater awareness of police violence by recording incidents on their phones, resulting in international awareness about the problem and the prosecution of certain offending officers. These technologies can be used to hold perpetrators accountable. However, with these opportunities come risks, **Karanasios** noted, begging the question, how can we support human rights defenders using these technologies to ensure that they are able to do so ethically, effectively, and safely? **Karanasios** emphasized the importance of engaging with technology companies, including social media companies, on these issues.

**Elsa Marie D’Silva, Founder, Red Dot Foundation (Safecity)**, described the power of technology in addressing inequality and driving community change. In 2012, after a young woman was gang raped in Delhi, India and later died of her internal injuries, **D’Silva** left a 20-year career in the Indian aviation industry to create an online platform called Safecity, which relies on anonymous crowdsourcing to document sexual harassment and abuse in public spaces. Safecity’s crowdsourcing effort allows anyone to anonymously share his or her story of sexual violence. See Figure 3 for an example of a Safecity crowdsourcing map.

**D’Silva** stressed that sexual violence is normalized in many parts of the world. This tends to lead to a data gap, where official statistics do not reflect the nature and size of the problem and, in turn, to an accountability gap. Safecity data help to illuminate the problem, allowing communities to understand it and



**Figure 3** Safecity crowdsourcing map. The numbers represent individual stories of sexual violence.

Source: From presentation by Elsa Marie D’Silva on Safecity

advocate for change (e.g., through education, engagement with police and religious leaders). According to **D'Silva**, involving communities in the process of creating such change is essential. This approach is low cost and replicable, demonstrating that individual and community action can drive institutional accountability. **D'Silva** emphasized that not everyone has access to technologies that can help to give them a voice, and that making efforts to expand such access is crucial. She also noted the importance of incorporating broader gender perspectives into technology, which she argued would improve technology overall.

**Keith Hiatt, Information Systems Management Section, United Nations International, Impartial and Independent Mechanism for Syria**, described the work of his office within the United Nations. In December 2016, the United Nations General Assembly adopted a resolution establishing the International, Impartial and Independent Mechanism, or IIIM, to assist in the investigation and prosecution of persons most responsible for serious crimes committed in Syria since March 2011. The IIIM has a mandate to collect, preserve, and analyze evidence of such crimes and to prepare case files with this evidence. Data are collected from a wide variety of providers, including civil society and member states, and come in many different formats. Analysis presents a major challenge for scientists, engineers, and health professionals, as data received do not always speak for themselves, and they often need to be connected to other types of data.

**Hiatt** noted that ensuring data are in a format that can be shared, as well as examining how to move digital assets from one place to another safely, is critical. Shipping certain kinds of data is extraordinarily dangerous, creating a vulnerability in the system. Science could play a role in figuring out how to facilitate secure information exchange. **Hiatt** concluded that the real challenge as we think about using data for accountability is less about creating new technologies than it is about developing the skill sets needed to support the technologies currently available, hiring people with those skills, and figuring out how to ensure that digital technology is designed/used in a manner that minimizes risks to individuals.

**Félim McMahon, Online Open Source Investigations Specialist**, stated that education related to the implications of digital technologies is a powerful way to deliver change; the National Academies are in a position to raise the visibility of this issue. Changes in information and communication technology and infrastructure over the past 25 years have transformed fact-finding and our world. These changes have created new possibilities, but have also produced harms, such as the spread of online disinformation.

**McMahon** discussed his prior work at University of California, Berkeley, in response to this concern, teaching an interdisciplinary group of 80, mostly undergraduate, students engaged in fact finding around human rights issues paired with civil society organizations. The ethical and practical issues that arose during this

work forced students to examine the digital world around them and consider it in new ways. Information is powerful, and the correct interpretation of it can have a transformative effect, **McMahon** said.

Internet platforms continue to play an important role in making more and more data available to the public and connecting individuals around the world. However, increasingly the online space is used to commit crimes and recruit individuals for such crimes. Addressing this problem is beyond the capacity of any one organization. Technology companies are beginning to respond to this problem, particularly in efforts to moderate and investigate problematic content on major platforms and increase liaison with law enforcement internationally. This needs to happen with openness and in a regulated, ethical way, **McMahon** concluded.

## CONTEMPORARY AND EMERGING CHALLENGES: DIGITAL TECHNOLOGIES AND HUMAN RIGHTS

**Shanthi Kalathil, Senior Director, International Forum for Democratic Studies, National Endowment for Democracy**, moderated a panel discussion on emerging challenges around digital technologies and human rights between **Alexa Koenig, Executive Director, Human Rights Center, University of California, Berkeley, School of Law**, and **Ron Deibert, Director, The Citizen Lab, University of Toronto**.

**Koenig** began by discussing the work of the Human Rights Center, which conducts multidisciplinary research on, among other things, human rights atrocities. A central piece of the Human Right Center’s work is to think about how new and emerging technologies can aid in investigating atrocities, in ways that will hold up in courts of law and public opinion. It includes a technology and human rights program, which in turn includes a lab composed of more than 80 students engaged in investigating/documenting human rights violations. The Human Rights Center consults with technology companies, conducts trainings on use of digital technologies, and is working to construct a protocol on open source investigations. It has also done research, for UNICEF among others, on the impact of AI-based technology on children.

**Deibert** introduced the work of The Citizen Lab at the University of Toronto, which does research on



**Figure 4** Shanthi Kalathil, National Endowment for Democracy; Alexa Koenig, University of California, Berkeley, School of Law; and Ron Deibert, The Citizen Lab, University of Toronto

Source: Cable Risdon/Risdon Photography



digital security issues arising out of human rights concerns. The Lab produces evidenced-based, peer-reviewed, reproducible research on internet censorship, surveillance, and targeted espionage. The Lab also engages in strategic high-level policy discussions, in an effort to help mitigate harms related to digital security. A serious concern relates to targeted digital attacks against civil society by governments using readily available commercial spyware, **Deibert** said.

The speakers discussed several key topics during the session:

### ***The power imbalance between civil society and government/corporate actors in the digital space***

**Deibert** noted that, although many individuals assumed that digital technologies would have a transformative effect in terms of promoting democracy and human rights, such technologies have in several ways made civil society more vulnerable to government abuses. This is partly because historical events (e.g., the war on terror, Arab Spring) caused many governments to seek access to new types of surveillance technology. The disclosures about U.S. government surveillance by Edward Snowden also unintentionally had this consequence. At the same time, individuals are increasingly vulnerable because much of our activity takes place on platforms not designed for security. A huge imbalance exists between the capacity of civil society and governments/corporations in the area of cyber-security. **Koenig** emphasized that the shift in roles of major social actors in this space requires much more mapping and thinking to fully understand its consequences. Going forward, **Koenig** said, we need to have a vision for the role of these actors, so that the ecosystem can be as healthy as possible.

### ***The need for multi-disciplinary research and training on digital technology and human rights***

**Koenig** discussed the need for more broad-based research and training on cyber-security, on mining data in a way that is ethical and responsible, and on the psycho-social impact of human rights fact-finding involving digital technologies. A multi-disciplinary approach is key, **Koenig** said, and we need to figure out how to incentivize collaboration across disciplines. **Deibert** argued that, as a matter of urgency, academics/universities should become more involved in multi-disciplinary research on the problem of use of digital technologies to undermine freedom of inquiry worldwide. Better protection is also needed for academics performing this type of research.

### ***Challenges related to informed consent***

**Deibert** indicated that The Citizen Lab has relied on research protocols and the research ethics board in Canada to help his staff think through how to interact with human subjects of research related to digital

technologies. **Koenig** pointed to challenges associated with informed consent when collecting data in conflict/crisis settings. In such settings, researchers should try to think through the possible risks, **Koenig** said, and communicate them to affected individuals in a way that can be understood—not only at the moment of data collection, but also over time. However, accurately assessing risks is often difficult.

**Koenig** expressed the view that the existing Institutional Review Board (IRB) system in the United States has limitations in such settings, which should be explored. According to **Koenig**, the IRB system was set up in response to ethical problems related to biomedical research—not social science research or other qualitative fact-finding investigations—and at a time that predates most digital communications. The digital environment raises new issues related to subjects' agency, informed consent, the balancing of risks and benefits, data storage, and other issues that are overdue for systematic analysis. **Koenig** observed that, as a result, there is little ethical guidance to support decision-making when engaging in fact-finding and other forms of research across social media platforms and other online spaces.

## RIGHTS, DISCRIMINATION, AND ARTIFICIAL INTELLIGENCE

**Mark Latonero (Panel Moderator), Research Lead for Human Rights, Data & Society**, outlined a number of efforts in 2018, including reports from [UN Special Rapporteur David Kaye, Harvard University](#), the [University of Essex, Data & Society](#), and several other nongovernmental organizations, to draw attention to issues surrounding human rights and artificial intelligence (AI). In early 2019, the Institute of Electrical and Electronics Engineers released a [report on ethically aligned design](#), which puts human rights as the first principle for ethical AI development and design. The European Commission released [Ethics Guidelines for Trustworthy AI](#), which include human rights, and the Council of Europe set up an expert committee that will include human rights as a legal basis for governing AI. Microsoft, Google, and Facebook have also made policy statements that include human rights. At the same time, we are continually seeing discrimination and other harms caused by AI systems, such as social biases associated with facial recognition particularly against people of color who are women. There is much at stake if we do not take action to address these harms, **Latonero** said, particularly for marginalized populations who are disproportionately impacted. Human rights can guide AI research, development, and deployment, but this requires instantiating human rights into the everyday practices, culture, and workflow of scientists, researchers, and others working on AI. Currently, experimenting with unproven AI applications on people is irresponsible and unregulated. **Latonero** also discussed the complementary, rather than contentious, relationship between ethical approaches and human rights frameworks for AI governance and pointed to the need for collaboration

between computer scientists and social scientists to assess and address AI-related harms.

**Eileen Donahoe, Executive Director, Global Digital Policy Incubator, Cyber Policy Center, Stanford University**, observed that much of the world now lives in AI-driven societies, where machine decision-making has infiltrated many aspects of life. **Donahoe** noted the risks of both inclusion and exclusion when it comes to digital technologies; this tension exists with AI. Although inclusion in the AI revolution raises many human rights concerns (see below for examples), she believes that *lack of inclusion* in this revolution is the dominant AI-related human rights concern at the moment because lack of inclusion has the potential to exacerbate other types of inequality.

**Donahoe** observed that, at the same time, we are in the midst of a geopolitical battle with respect to the norms that will guide regulation of AI. One concern is a global unconscious drift toward digital authoritarianism. This applies even to democratically-oriented countries. AI also has the potential to displace humans as the focal point in society and creates problems in terms of accountability for decision-making. It is important, in response, to advocate for use of the existing international human rights framework (international human rights treaties and implementation mechanisms) to govern AI. Although this framework isn't perfect, it guarantees the centrality of the human person and provides a foundation for governments, industry, and civil society to help ensure rights protection while reaping the benefits of digital technologies. Many stakeholders in this area are not familiar with international human rights law; some are moving to develop ethical principles without understanding that they are contributing to erosion of the international human rights framework. According to **Donahoe**, we have a lot of hard work ahead to articulate in a compelling way how international human rights applies with respect to freedom of expression, freedom of assembly, the right to privacy, equal protection, and non-discrimination in the digital age. This needs to be a cross-disciplinary, multi-stakeholder process.



**Figure 5** Kristian Lum, Human Rights Data Analysis Group; Rashida Richardson, AI Now Institute, New York University; and Eileen Donahoe, Cyber Policy Center, Stanford University

Source: Cable Risdon/Risdon Photography

**Rashida Richardson, Director of Policy Research, AI Now Institute, New York University**, discussed concerns related to AI and discrimination, particularly in connection with the data used in AI. It is often presumed that data are objective and accurately reflect reality. However, this is not the case, given current data collection and use practices. The data used in AI can have the effect of normalizing the unequal status

quo. If we assume data are objective, many of the problems we are seeing with AI will not be addressed; the technology will perpetuate problems in society. For example, race and zip code are correlated in the United States based on a long history of discrimination. Many AI systems will not discern this problem, making it more difficult to respond effectively, **Richardson** observed. Our current legal frameworks are not enough; they need to evolve along with this rapidly evolving technology.

**Kristian Lum, Lead Statistician, Human Rights Data Analysis Group**, stated that AI systems can launder bias in data, resulting in future bias. **Lum** illustrated the problem by applying a predictive policing algorithm, similar to one used in the real world, to a dataset on drug crimes in Oakland, California. The algorithm did not take race into account; it only considered information about past crimes. Nevertheless, it reproduced a pattern of over-enforcement in African-American and Hispanic neighborhoods. Training the algorithm with other types of data, such as public health surveys, would have produced a very different outcome. **Lum** also suggested that we think about whether we should even be using certain algorithmic systems, such as facial recognition tools.

## **FAIRNESS AND PRIVACY: GAINS AND LOSSES IN THE DIGITAL AGE**

**Cynthia Dwork, Gordon McKay Professor of Computer Science, John A. Paulson School of Engineering and Applied Sciences, Harvard University**, described her work to develop theoretical computer science as a vehicle for social change. As an example of unfairness associated with algorithms, she cited problems associated with facial recognition systems, including in recognizing the faces of African-American women. **Dwork** noted that algorithms underlying such systems use training data that contain historical biases.

**Dwork** outlined theories of algorithmic fairness, explaining that group fairness notions fail under scrutiny. Individual fairness, which requires that people who are similar with respect to a given classification task should be treated similarly, gives rise to a powerful mathematical framework, but this also raises questions. How, for instance, do we determine the right task-specific notion of similarity for a pair of people? Some progress has recently been made in this area. Innovative work is also being done looking at models in between group and individual fairness. In this realm, certain group fairness requirements are imposed on a collection of large, intersecting, subsets of the population. For example, the requirement for a scoring function might be that it is (approximately) correct on average for each group simultaneously.

**Dwork** also presented the concept of differential privacy, which ensures that the outcome of any analysis is essentially equally likely, independent of whether any individual joins or refrains from joining the dataset.

It operates by adding carefully generated noise at certain points in the calculations. For the first time in 2020, differential privacy will be used as the disclosure control mechanism for the decennial census. This is meant to address privacy issues arising from the prior census, where it was possible to reconstruct information from data tables that were previously assumed to be privacy preserving. A general challenge in differential privacy is that researchers are not trained to interact with data in a differentially private way. **Dwork** noted that more research is needed to understand how differential privacy might be used for generating synthetic data with high-dimensionality.



**Figure 6** Cynthia Dwork, Harvard University

Source: Cable Risdon/Risdon Photography

**Chalfie** concluded the symposium by expressing his gratitude to presenters. The human rights challenges related to digital technologies present an opportunity for scientists and engineers to contribute to the development of what was referred to by **Berens** as “value sensitive and rights based technologies.” This requires, among other things, listening to the voices of the intended beneficiaries of digital technologies. It also requires greater collaboration between the scientific/technology community and human rights experts. Unfortunately, these groups often see themselves as speaking different languages. The continuing gaps and siloes in this area support the call for greater emphasis on human rights education, **Chalfie** stated, and integration of human rights into STEM higher education.

**DISCLAIMER:** This Proceedings—in Brief was prepared by **Jennifer Saunders** as a factual summary of what occurred at the meeting. The statements made are those of the rapporteur or individual meeting participants and do not necessarily represent the views of all meeting participants or the U.S. National Academies of Sciences, Engineering, and Medicine.

**MODERATORS AND SPEAKERS:** **Jos Berens**, Data Policy Officer, United Nations Office for the Coordination of Humanitarian Affairs (OCHA); **Jessie Brunner**, Senior Program Manager, Center for Human Rights and International Justice, Stanford University; **Martin Chalfie**, University Professor, Columbia University and Chair, Committee on Human Rights, U.S. National Academies of Sciences, Engineering, and Medicine; **Ron Deibert**, Director, The Citizen Lab, University of Toronto; **Eileen Donahoe**, Executive Director, Global Digital Policy Incubator, Cyber Policy Center, Stanford University; **Elsa Marie D’Silva**, Founder, Red Dot Foundation

(Safecity); **Cynthia Dwork**, Gordon McKay Professor of Computer Science, John A. Paulson School of Engineering and Applied Sciences, Harvard University; **Keith Hiatt**, Information Systems Management Section, United Nations International, Impartial and Independent Mechanism for Syria; **Shanthi Kalathil**, Senior Director, International Forum for Democratic Studies, National Endowment for Democracy; **Tanya Karanasios**, Deputy Program Director, WITNESS; **David Kaye**, United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; **Alexa Koenig**, Executive Director, Human Rights Center, University of California, Berkeley, School of Law; **Mark Latonero**, Research Lead for Human Rights, Data & Society; **Kristian Lum**, Lead Statistician, Human Rights Data Analysis Group; **Félim McMahon**, Online Open Source Investigations Specialist; **Dani Poole**, Postdoctoral Fellow, Harvard Humanitarian Initiative, Harvard University; **Nathaniel Raymond**, Lecturer, Jackson Institute of Global Affairs, Yale University; **Rashida Richardson**, Director of Policy Research, AI Now Institute, New York University.

Note that not all voices from human rights practices are reflected in this Proceedings—in Brief.

**STAFF:** **Rebecca Everly**, Director, Committee on Human Rights; **Patricia Evers**, Deputy Director; **Tracy Sahay**, Associate Program Officer; and **Ana Deros**, Senior Program Assistant.

**REVIEWERS:** To ensure that it meets institutional standards for quality and objectivity, this Proceedings—in Brief was reviewed by **Brandie Nonnecke**, University of California, Berkeley; **Jason Pielemeier**, Global Network Initiative; and **Enrique Piracés**, Carnegie Mellon University.

For additional information regarding the activities of the Committee on Human Rights, visit <https://www7.nationalacademies.org/humanrights/>.

Suggested citation: Committee on Human Rights of the National Academies of Science, Engineering, and Medicine. 2020. *Human Rights and Digital Technologies: Proceedings of a Symposium of Scholars and Practitioners—in Brief*. Washington, DC.

### Committee on Human Rights

*The National  
Academies of* | SCIENCES  
ENGINEERING  
MEDICINE

The nation turns to the National Academies of Sciences,  
Engineering, and Medicine for independent, objective advice  
on issues that affect people's lives worldwide.

Copyright 2020 by the National Academy of Sciences. All rights reserved.