Data&Society

Data, Human Rights & Human Security

Primer 06.22.2015

MARK LATONERO, PhD—Fellow and Principal Investigator

ZACHARY GOLD, JD—Research Analyst

Introduction

In today's global digital ecosystem, mobile phone cameras can document and distribute images of physical violence. Drones and satellites can assess disasters from afar. Big data collected from social media can provide real-time awareness about political protests. Yet practitioners, researchers, and policymakers face unique challenges and opportunities when assessing technological benefit, risk, and harm. How can these technologies be used responsibly to assist those in need, prevent abuse, and protect people from harm?

For some years now, the humanitarian and development communities have explored new data-driven approaches, innovations, and interventions.[1] However, for human rights and human security decision-makers distinct questions emerge, particularly when collecting personal data for case analysis and protection beyond crisis events. Releasing cell phone data might assist first responders to track disease outbreaks. But should the same data be shared for long-term issues such as human

1 *See* Big Data for Development: Opportunities and Challenges, UN Global Pulse (2012), http://www.unglobalpulse.org/projects/BigDataforDevelopment; Disaster Relief 2.0, UN Foundation http://www.unfoundation.org/assets/pdf/disaster-relief-20-report.pdf; Key Resources, Data Pop Alliance, http://www.datapopalliance.org/resources#start.

trafficking? Collecting aggregate population data can inform economic policies on poverty. Yet what about mining those data sources to personally identify someone who is at immediate risk of gender-based violence?

Data and information have always been important for these fields. What is new is the evolving nature of data, which springs from an array of digital technologies – from social media and mobile devices to the Web and Internet of Things. Massive amounts of data can be stored and analyzed through advances in search, pattern recognition, and visualization. Data can be collected in real time, shared (or intercepted) in an instant, and persist over time. In addition, social factors cannot be separated from data or the interpretation of data. Raw data, for example, fundamentally comes with social biases and assumptions. In the case of networked data, information collected from one person can reveal social relationships and characteristics about others unbeknownst to them.

Can the data-driven technologies that are transforming various aspects of our commercial and social lives have the potential to address human suffering, empowerment, and justice? The problem is that we simply do not know all the positive and negative impacts these new technologies will bring, which makes it difficult to make informed decisions in the present. We do not yet know how data science, computation, and design thinking might influence traditional legal, interventionist, economic, and protectionist frameworks.

To understand how cutting-edge technological innovation can be applied in the human rights and security arenas often requires cross-disciplinary "translation" work. Human rights experts may not have the vocabulary to convey their "asks" to engineers or statisticians. Similarly, software developers may know little about consequences to vulnerable populations. A translator or broker is often needed for diverse actors to establish a baseline understanding around data, evaluate the efficacy of emerging technologies, and develop actionable strategies. Ideally, stakeholders would coordinate to develop evidence-based guidelines and policies before data interventions are applied in the field. Deploying new tools without appropriate safeguards – even when the situation calls for a rapid response – can increase risk to beneficiaries.

This primer seeks to highlight and anticipate the emergent complexities at the intersection of data, human rights, and human security. More tensions and questions than definitive answers are identified below and some concepts blur into others. That is to say, this primer argues that more foundational work and leadership is needed in this area. Indeed, these issues should be addressed early and systematically, before well-intentioned data-driven interventions fail to assist—or even harm—

intended beneficiaries. Eventually, common frameworks and guiding principles will need to come from this field of research in order for stakeholders across sectors to accelerate data benefits and mitigate risks. Naturally, overlap exists in current efforts to establish responsible data guidelines from intergovernmental organizations, NGOs, business, and researchers.[2] Integrating human rights and security perspectives should make for a more robust conversation.

Key Issues/Tensions

Accuracy, Validity, & Prediction: How should data analytics be used to make decisions in human rights and security domains?

New technologies enable awareness (and potential intervention) into the physical, social, and political environment more quickly than ever before. Analytic tools can filter through huge amounts of data to find signals of potential threats and identify individuals in need.[3] However, big data analysis deals in possible correlations, not causation nor objectivity. Serious concerns about sampling, representation, and population estimates call into question the utility of big data in policy making.[4] Moreover, all big data sets give a biased view of reality as individuals and attributes will be excluded. New requirements for disclosing biases may be needed to alert decision-makers to avoid hasty generalizations.

The notion of substituting big data inferences for deep expertise and judgment raises particular concerns where the consequences to human lives are paramount. Data gathered from crowdsourcing, social media, and mobile phones can give unprecedented insight for individual case analysis. But can this data used for policy making and resource allocation? Quantitative analysis from big data can provide the "scaffolding" that builds up a case. But is qualitative research ultimately necessary to verify evidence? Predictive modeling of potential violations or abuses may be new for some in the human rights community. Yet human security organizations have used predictive techniques for crisis and conflict modeling for some time. Large troves of data allow for new kinds of decision-making and

---

[2] Responsible Development Data Book, Responsible Data Forum (2015), https://responsibledata.io/ways-to-practise-responsible-development-data/; Humanitarian Connectivity Charter, GSMA (2015), http://www.gsma.com/newsroom/press-release/gsma-launches-humanitarian-connectivity-charter/; Data-Driven Development, World Economic Forum, http://www3.weforum.org/docs/GAC/2013/Connect/WEF_GAC_Data-Driven_Development_2012-2014_Connect.pdf; *See also*, Resources, Responsible Data Forum, https://responsibledata.io/category/resources/.

[3] See, e.g., Mark Leon Goldberg, How Big Data Can Put War Criminals Behind Bars, UN Dispatch (March 17, 2014), http://www.undispatch.com/we-gov-piece/.

[4] Patrick Ball, Digital Echoes: Understanding Patterns of Mass Violence with Data and Statistics, Presented to a meeting at the Open Society Foundations, New York, NY (May 2015).

enable predictions about future actions. The potential for human rights observers to predict violations such as mass atrocities suggests a unique paradigm where preventive measures can be implemented instead of documenting and intervening after the fact. Yet predictive models based on big data are prone to error. What types of data are appropriate in what contexts? What are the appropriate threshold levels of acceptable error for human rights and security?

Data-driven monitoring and modeling of human rights abuses may capture previously unobserved phenomena, but may also generate false positives or false negatives. For example, one statistical model claims to predict about 80 percent of political coups in a given year.[5] Even if this rate is accurate, it is cold comfort to the citizens in the countries that the model missed. It remains unclear what interventions are appropriate based on types of data or acceptable error. Who is responsible for actions based on inaccurate data, models, or predictions?

Risks, Harms, & Benefits:
What risks and benefits frameworks will guide decision makers about data-driven interventions?

Kranzberg's first law of technology states, "technology is neither good nor bad; nor is it neutral." Advocates, researchers, and policymakers can use new technologies and big data to better understand the contours of state repression or human rights abuses. An increasingly open and connected world should make it more difficult for authoritarians to repress in secret. For example, Google Earth and the United States Holocaust Museum partnered to capture satellite data of the Darfur crisis.[6] Amnesty International and the American Association for the Advancement of Science have similarly used geospatial technologies to detect atrocities in Syria.[7]

Tools that shed light on repressive regimes may, in the wrong hands, be used to monitor and repress those who challenge the state.[8] For example, in the Syrian conflict, fake Facebook and Twitter login pages were created to capture the personal information of dissidents organizing on the internet.[9]

---

5 Jay Ulfedlder, A New Statistical Approach to Assessing Risks of State-Led Mass Killing, Dart-Throwing Chimp, https://dartthrowingchimp.wordpress.com/2014/01/22/a-new-statistical-approach-to-assessing-risks-of-state-led-mass-killing/.

6 Crisis in Darfur, United States Holocaust Memorial Museum (2009), http://www.ushmm.org/learn/mapping-initiatives/crisis-in-darfur.

7 Satellite Images of Aleppo, Now Half-Emptied, Show Devastation, Amnesty International (Aug. 7, 2013), https://www.amnestyusa.org/news/press-releases/satellite-images-of-aleppo-now-half-emptied-show-devastation.

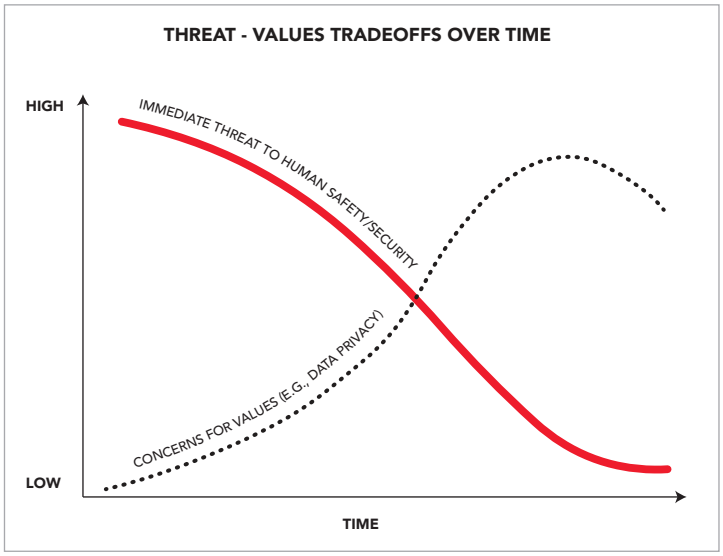
8 See generally, Christoph Koettl, Tech and Human Rights: The Good, The Bad, and The Ugly, Amnesty International (March 19, 2015), http://blog.amnestyusa.org/europe/tech-and-human-rights-the-good-the-bad-and-the-ugly/.

9 The Syrian Conflict in a Connected World, Council on Foreign Relations (June 20, 2013), http://www.cfr.org/content/publications/attachments/Syrian_Conflict_in_a_Connected_World_Rapporteur_Notes_7-2-13.pdf.

Harms from data revelations range from physical violence, to retribution, to shaming. Yet a more precise taxonomy of data related harms is needed. Metrics are needed to inform decisions based on data risks, harms, and benefits. Who has the authority to make these decisions? When should privacy impact assessments be mandated (and enforced) either by government[10] or self-regulatory mechanisms? Can these decisions be embedded into the design and development of data-centric technologies and software?[11]

Balancing Immediate Threats & Values: Should values like privacy fluctuate in the face of immediate threats?

Immediate threats to people's lives can create tensions between core values around data. The graph below depicts one tradeoff model (among many) between threats and values over time. For example, during the immediate response to the Ebola outbreak, information such as individual names, characteristics, photographs, and addresses were circulated to aid workers trying to contain the spread of the virus.[12] During times of extreme crisis the concern over data privacy may be low (see dotted line). But as the threat to life diminishes over time, the value of privacy concerns increases. But not all situations follow this model. After the crisis phase for Ebola, some survivors were stigmatized and left vulnerable. Indeed, the very act of collecting or sharing data can increase the risk of violence or retribution. In other scenarios,



10 Privacy Impact Assessments Official Guidelines, U.S. Department of Homeland Security (May 2007), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.

11 Data Collection in Humanitarian Response, Responsible Data Forum, http://pqdl.care.org/Practice/Data%20Collection%20in%20Humanitarian%20Response,%20A%20Guide%20for%20Incorporating%20Protection.pdf.

12 For opinions on Ebola as a human security issue, see: Maryam Zarnegar Deloffre, Will AFRICOM's Ebola response be watershed moment for international action on human security? The Washington Post (Sept. 29, 2014), http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/09/29/will-africoms-ebola-response-be-watershed-moment-for-international-action-on-human-security; Human Security in the Age of Ebola: Towards People-centered Global Governance, E-International Relations (Oct. 25, 2014), http://www.e-ir.info/2014/10/25/human-security-in-the-age-of-ebola-towards-people-centered-global-governance/.

privacy concerns can remain high in relation to threats over time. In the perspective of some stakeholders, like first responders, their operational mode is only the high threat realm, while others have a multi-year horizon for a particular issue or geographic area.

Such tradeoffs require measured assessments, which are often unclear and ambiguous when data is readily available, easy to collect, or simple to share. An abundance of caution may protect privacy interests, but could hinder aid efforts. How should rights and security officials measure values like data privacy against threats to those they have a responsibility to protect?

Adaptation/Unintended Consequences: How will data collection and monitoring shape the practices of those that repress or advocate for human rights?

Advanced data collection and data mining techniques can alter how human rights situations are monitored and witnessed. Just as citizens may internalize and adjust their behavior to avoid government systems of surveillance,[13] authoritarian regimes might pursue less visible forms of repression and abuse in response to the changing landscape of human rights monitoring. Research suggests "clean torture" techniques that minimize visible evidence of torture are a consequence of increased scrutiny on the state, which finds new ways to evade detection.[14] At the same time, human rights activists may need to act with more care, as safe spaces may be targeted by repressive regimes.[15] What forms of abuses or repression will remain invisible in the digital environment? How might the introduction of data-centric technologies or techniques inadvertently cause harm to intended beneficiaries?

Governance & Accountability: How can data regulation, policy, and standards effectively govern and provide accountability?

It is incumbent on policymakers to seek guidance on emerging data ethics, laws, and policies. Governance and accountability might come in forms such as industry ethics boards, new intergovernmental policies, or the reevaluation of current national laws. For example, some evidence

---

13 Sarah Brayne, *Surveillance and System Avoidance*, American Sociological Review (2014), *available at*, https://www.academia.edu/9565513/Surveillance_and_System_Avoidance_Criminal_Justice_Contact_and_Institutional_Attachment.

14 Darius Rejali, *Torture and Democracy*, Princeton University Press (2009).

15 *An Invisible Threat: How Technology Can Hurt Human Rights Defenders*, Amnesty International (Nov. 11, 2013), http://blog.amnestyusa.org/middle-east/an-invisible-threat-how-technology-can-hurt-human-rights-defenders/.

gathered using new technologies is not admissible in national courts or international tribunals. In 2013, Amnesty International declared an "urgent need for guidelines on the reliability and admissibility rules of social media and video evidence."[16]

Governments and international bodies, such as the European Court of Human Rights, have also begun to explore how personal data should be balanced in light of conventions on civil and human rights.[17] How will privacy as human right reconcile with rights to data ownership or freedom of information? Who is accountable when bad decisions are based on algorithms? What is the value of accountability principles like transparency when big data algorithms are increasingly complex and opaque?

Collecting, Sharing, & Security: How should human rights and human security data be responsibly collected, stored, secured, and shared?

Concerns regarding the collection, security, and availability of sensitive data on vulnerable populations are nothing new. Yet, it is important for human rights and security professionals to understand that digital environments create new vulnerabilities from mishandling or cyberattacks. Some human rights interventions rely on a "truth and reconciliation" framework that emphasizes the public disclosure of human rights violations and repression. On the other hand, inadvertently releasing data can result in irrevocable harm. If an adversary such as a perpetrator of abuse gains access to sensitive information on a victim the consequence can include acts of violence or retribution. Human rights workers will need to avoid breaches or misuse of the data that they collect, use, analyze, and store.[18] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stressed the importance of privacy, encryption, and anonymity in forwarding basic human rights.[19] Journalists reporting on human rights abuses or serving as government watchdogs are also key beneficiaries of better encryption tools.[20] Where do

---

16 *Twitter to the Rescue? How Social Media is Transforming Human Rights Monitoring*, Amnesty International (Feb. 20, 2013), http://blog.amnestyusa.org/middle-east/twitter-to-the-rescue-how-social-media-is-transforming-human-rights-monitoring/.

17 Patrick Eggimann & Aurelia Tamò, *Taming the Beast: Big Data and the Role of Law*, Future of Privacy Forum, http://www.futureofprivacy.org/wp-content/uploads/Eggimann-Tamo-Taming-the-Beast-Big-Data-and-the-Role-of-Law.pdf.

18 *The Madrid Resolution, International Standards on the Protection of Personal Data and Privacy*, International Conference of Data Protection and Privacy Commissioners (Nov. 5, 2009), http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf.

19 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council (2015), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

20 Kelly J. O'Brien, *How journalists should reframe the encryption debate*, Columbia Journalism Review (Feb. 26, 2015), http://www.cjr.org/behind_the_news/how_journalists_are_fighting_t.php.

cybersecurity,[21] privacy, and encryption intersect with human rights and human security?

If the demand or dependency for data derived from new technologies becomes more widespread, the "data-driven" mantra might start to shape project design, workflows, or practices in human security and human rights fields. At the same time, practitioners should ensure that data collection is proportional, accurate, and confidential, and that use of the data is legitimate, fair, and accountable. Furthermore, citizens or beneficiaries are often not aware their data is being collected. Obtaining consent from those whose data is being collected is already a fraught issue[22] and adding a human rights or security element adds to the debate.[23] Should informed consent be reexamined? Do privacy concerns apply to data collected from openly available sources online? When should the amount and kind of data collection be maximized or minimized for vulnerable populations? How long should data be retained? How should risk be assessed for data that cannot be fully anonymized? How can technologies help ensure shared data is used for legitimate purposes?

The protocols and practices around data sharing across private and public sectors are only beginning to be discussed. Do private sector actors who collect and sell commercial data have a responsibility to share data with human rights and human security officials? How can advances in encryption facilitate the sharing of sensitive data or inadvertently increase vulnerability?[24] How can encryption tools, such as Tor, secure data and communications in rights and security contexts?[25]

Aggregation vs. Identification: How should the human rights and human security fields interact with data tools and techniques that can identify specific individuals at risk?

In contexts such as data for development, aggregate population statistics can be used to make policy decisions affecting large numbers of beneficiaries. Yet human rights and security interventions can

---

21 For the intersection between cyber-warfare and humanitarian action see UNOCHA https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf.

22 Fred H. Cate & Viktor Mayer-Schonberger, *Notice and consent in a world of Big Data*, 3 Int'l Data Privacy Law, Issue 2 (2013), http://idpl.oxfordjournals.org/content/3/2/67.abstract.

23 Kathy Wren, *Big Data and Human Rights, a New and Sometimes Awkward Relationship*, AAAS (Jan. 28, 2015), http://www.aaas.org/news/big-data-and-human-rights-new-and-sometimes-awkward-relationship (Samir Goswami, director of Government Professional Solutions at LexisNexis, discussing the problems of informed consent and unknown future uses of data in human rights).

24 Patrick Ball, *When It Comes to Human Rights, There Are No Online Security Shortcuts*, Wired (Aug. 10, 2012), http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/.

25 *Users of Tor*, Tor, https://www.torproject.org/about/torusers.html.en.

operate at a small scale or individual case level. If a data set contains a signal that an individual is actively being exploited or is in immediate danger, practitioners must decide whether that individual should be identified. Does the opportunity to provide assistance outweigh the possible consequences of revealing personal information? How great a harm should the person face in order to justify an invasion of privacy, and should uncertainty as to the field's ability to actually provide assistance affect the decision? Finally, who makes these decisions and how can they be approached responsibly?

Context & Power Dynamics:
Can general guidelines and principles be established for data interventions whose social applications are deeply contextual and enmeshed in power relationships?

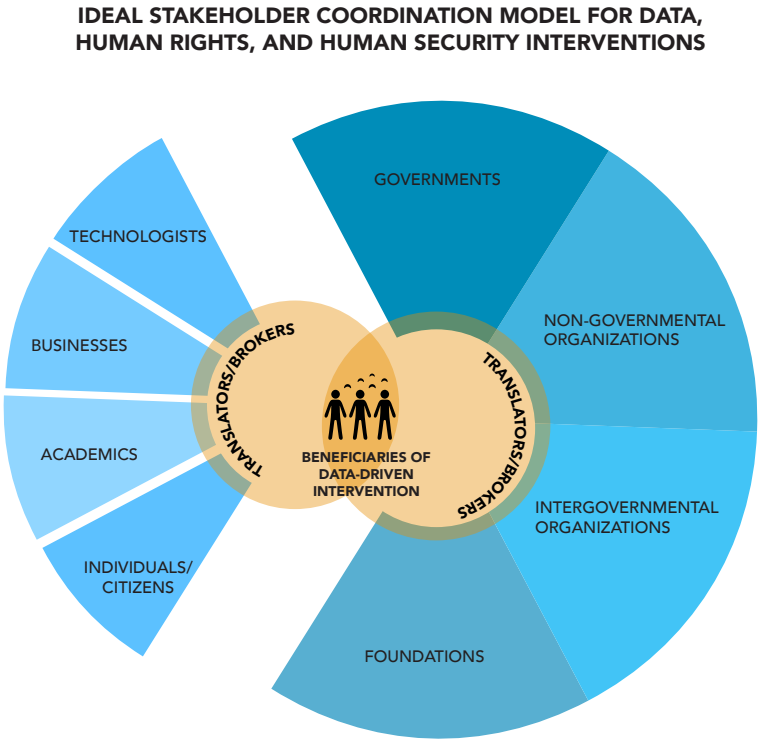
Through policy discussions and case studies, experts can derive general frameworks and guiding principles for future data interventions. However, there is a possibility that no standards can be generalized, given that each intervention occurs within a particular culture, time, and place. In some locations, the technological infrastructure may not support the tool. Types of data, like call detail records, may be owned by the State rather than a private entity. Data-driven interventions may be met with suspicion in locations impacted by colonial oppression, repressive State surveillance, or mistrust of foreign corporations. The very introduction of data-centered technologies can both reveal and exacerbate power relations and asymmetries such as mapping tools that could unexpectedly make political affiliations visible. Technologists and subject matter experts might anticipate unforeseen outcomes by including the voices of intended local beneficiaries into the design and engineering of data-centered interventions. How might interventions reinforce existing structural conditions like racism or gender discrimination? Who are data-centered technologies ultimately empowering or disempowering?

Stakeholders

The introduction of new technologies brings new stakeholders, issues, and responsibilities to the table. As technologies intended for one purpose are deployed to other domains, their use might lack context specific values and the potential impact may be uncertain. It is critical that actors coordinate across organizations and disciplines to evaluate benefits, threats, adversaries, and risks. Technology firms, academic computer scientists, or software developers whose work appears unrelated to human rights could have data and analytic tools that could help practitioners monitor or protect human rights and security. Human rights organizations could benefit tremendously from these resources but need to

understand the limitations and risks.

Traditional stakeholders now face decisions on whether integrating data-centric technologies — or



Translators and brokers serve to connect both within and across stakeholder groups to develop responsible actions.

even hiring a data scientist — will advance or detract from their primary objectives and missions.

The graphic above represents an ideal model for incorporating both new and traditional stakeholders to coordinate around data-driven interventions. Translators and brokers serve to connect both within and across stakeholder groups to develop a common understanding of technological approaches and responsible actions. People-centered human security and rights frameworks place beneficiaries as the ultimate focal point of any data-driven intervention.

NGOs

Nongovernmental organizations have long served as "information brokers" in the human rights space.[26] These actors have traditionally monitored rights and security conditions locally and internationally, and pressured state power to act upon their findings. In a data-saturated world, these entities face decisions like whether to crowd-source online data,[27] use remote sensing technologies, or to deploy staff "on the ground."[28] These organizations must decide how to integrate these new techniques with traditional forms of information gathering. Where they do rely on new data collection technologies, they should address issues like validity, bias, evidence, and security. Expertise in data, statistics, and analytics are often needed to bridge the knowledge gap between technological application and the deep contextual knowledge of subject matter experts.

Academia/Non-profit Research

Academics have generated and analyzed data on human rights and human security through indices like the Political Terror Scale[29] and the Human Rights Data Project.[30] Researchers from the Human Rights Data Analysis Group (an independent non-profit) are creating innovative statistical techniques to document and estimate human rights violations.[31] Recently, data mining projects from social media and print journalism collect large disaggregated data on previously obscured human rights phenomena.[32] Academic research can produce rigorous results that can advance many aspects of human rights and security work. However, those who might cite or utilize these studies must carefully consider the scope, methodology, and limitations before making policy or operational decisions.

A number of academic advances in computer and data science can assist in the human rights and security fields, such as machine learning, artificial intelligence, natural language processing,

---

26 Michael Stohl & Cynthia Stohl, *Human Rights, Nation States, and NGOs: Structural Holes and the Emergence of Global Regimes*, 72 Communication Monographs 4 (2005), http://www.tandfonline.com/doi/abs/10.1080/03637750500322610?journalCode=rcmm20.

27 Stefaan Verhulst, *Crowdsourcing the monitoring of human rights violations*, Govlab (March 26, 2013), http://thegovlab.org/crowdsourcing-the-monitoring-of-human-rights-violations; *Checklists for verifying user-generated content*, Responsible Data Forum, https://responsibledata.io/checklists-for-verifying-user-generated-content/.

28 *Remote Sensing for Human Rights*, Amnesty International, http://www.amnestyusa.org/research/science-for-human-rights/remote-sensing-for-human-rights.

29 Political Terror Scale, http://www.politicalterrorscale.org/.

30 CIRI Human Rights Data Project, http://www.humanrightsdata.com/.

31 *Publications*, Human Rights Data Analysis Group, https://hrdag.org/publications/.

32 *Human Rights Coverage Over Time: A Tutorial in Automated Text Analysis*, D-Lab, http://dlab.berkeley.edu/blog/human-rights-coverage-over-time-tutorial-automated-text-analysis.

visualization, vision, distributed processing, cybersecurity, search, and classification. As these new academic actors conduct applied research in human rights or security fields it is incumbent upon them to seek an understanding of the social consequences of their discoveries. For example, researchers can apply modeling techniques to predict human rights crises, often advising governments and intergovernmental organizations on how to best focus their efforts.[33] Yet, the transfer of technology from academia to stakeholders heightens the debate surrounding the ethics, use, and purpose of data research.[34] A laboratory environment can provide a space for experimentation with technologies and human rights and security,[35] yet application in the field is ultimately necessary. Including human rights and security subject matter experts at the earliest stages of scientific research and development (i.e. practice-informed project design) can mitigate unintended consequences to beneficiaries.

Private Sector

The technology sector has unparalleled expertise and access to talent, raw data, storage, and advanced analytics. Business has the resources and capacity to conduct basic research and development, test ideas, and bring them to market. But design and development workflows that encourage iteration and failure could result in grave consequences in the rights and security contexts. It is also not new that the same products companies view as socially beneficial may be used by those in power to facilitate human rights abuses.

Business has unique responsibilities to "protect, respect, and remedy" according to the UN Human Rights Council.[36] The technology sector should explore innovating in keeping with this framework. In recent years, "data philanthropy" has emerged as a model by which the private sector can share data for social good.[37] Such models serve to align incentives for business to responsibly leverage their data

---

33 Early Warning Project, http://www.earlywarningproject.com/.

34 Erik Voeten, *Can forecasting conflict help to make better foreign policy decisions?*, The Monkey Cage (July 28, 2013), http://themonkeycage.org/2013/07/28/32299/; Jay Ulfelder, *Yes, Forecasting Conflict Can Help Make Better Foreign Policy Decisions*, Dart-Throwing Chimp, https://dartthrowingchimp.wordpress.com/2013/07/29/yes-forecasting-conflict-can-help-make-better-foreign-policy-decisions/; Lilli Japec, Frauke Kreuter, et al., *AAPOR Report on Big Data*, American Association for Public Opinion Research (Feb. 12, 2015), https://www.aapor.org/AAPORKentico/AAPOR_Main/media/Task-Force-Reports/BigDataTaskForceReport_FINAL_2_12_15_b.pdf; Seth Young, *Sloan Foundation funds Ethics in Data Research exploratory project*, Data & Society (May 19, 2015), http://www.datasociety.net/blog/2015/05/19/sloan-foundation-funds-ethics-in-data-research-exploratory-project; Council for Big Data, Ethics, and Society, http://bdes.datasociety.net/.

35 *See* University of Leiden Peace Informatics Lab, http://www.peaceinformaticslab.org/.

36 For more on the "Ruggie principles," *see*, *Guiding Principles on Business and Human Rights*, United Nations Human Rights Office of the High Commissioner (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

37 *See* Matt Stempeck, *Sharing Data Is a Form of Corporate Philanthropy*, Harvard Business Review (July 24, 2014), https://hbr.org/2014/07/sharing-data-is-a-form-of-corporate-philanthropy; *Responsible Data Forum on Private Sector Data Sharing*, UN Global Pulse, Data & Society, & The Engine Room (2014), *available at*

assets to addresses crucial global issues. Yet, concerns over ownership of data, dependency, and power relationships between data businesses and consumers loom large. To ensure safeguards and mitigate unintended consequences, technology companies seeking to enter into the human rights or human security spaces should seek counsel from a range of stakeholders.[38]

Technologists

Technologists, dispersed across sectors and organizations, can provide much needed skills towards human rights and security projects. In fact, a growing number of professional data scientists, software developers, or computational statisticians are organizing around the impetus to "do good." They might participate in hackathons, serve as consultants on government funded projects, or become hired in-house by traditional stakeholders. The tools and software they develop could be used to intervene in any number of human rights or security issues. Yet it is unlikely technology itself will provide a silver bullet solution to long-standing social, historical, structural, or contextual problems.[39] Often the social barriers to addressing these issues are far more important than technological ones. Technologists should understand the ethics and responsibilities of applying technologies in areas where they lack expertise. They should seek guidance from a diverse set of stakeholders in order to understand the politics and conflicts within the space. For example, one stakeholder can be a good actor in one national context and a repressive force in another. Lastly, technologists can implement safeguards like user agreements and privacy-by-design into the technologies themselves.

Governments and Intergovernmental Organizations

Intergovernmental organizations are uniquely positioned to convene stakeholders and create policies that incentivize the development and implementation of data-centered technologies in human rights and security contexts. IGOs can address policy barriers to innovation, including reevaluating evidentiary standards that do not account for new sources of data on human rights violations or intellectual property concerns over privately held information that could mitigate a human security

http://www.datasociety.net/blog/2014/08/25/responsible-data-forum-on-private-sector-data-sharing/; Robert Kirkpatrick, *A New Type of Philanthropy: Donating Data*, Harvard Business Review (March 21, 2013), http://blogs.hbr.org/2013/03/a-new-type-of-philanthropy-don/.

38 Center for Business and Human Rights, New York University, http://www.stern.nyu.edu/experience-stern/about/departments-centers-initiatives/centers-of-research/business-and-human-rights. *See also*, *Data Governance Project*, University of Leiden Peace Informatics Lab, www.peaceinformaticslab.org/data-governance-project.

39 *See* Kentaro Toyama, Geek Heresy: Rescuing Social Change from the Cult of Technology (2015), http://geekheresy.org/.

crisis.[40]

Governments can coordinate new research and development on data innovations to enhance their human rights and security programs. States can also use data collection and analysis for human rights through diplomacy, or sanctions, or interventions. New technologies and data influence states' interventionist decision-making by providing them with more – but not necessarily more accurate – situational awareness. As security experts within government rely on new data and advanced forecast models to assess the necessity of intervention, they should be prepared to handle statistical uncertainty and risk.[41] One vexing problem is how to safeguard against governments using new data innovations developed for human rights concerns and repurposing them into tools for political repression.

Foundations

Foundations can set an agenda for human rights organizations around responsible data practices and tools. As the human rights and human security fields become more data-intensive, foundations can invest in medium to long term research and development for safe and effective data centric technologies. Enabling activists and advocates to use and adapt technologies for human rights could require resources and capacity to explore social and technical solutions before they are tested in the field.

Foundations may use new technologies and data to make decisions about where to focus their resources or to evaluate the performance of the organizations and initiatives. In doing so, they should adapt their decision-making processes to take into consideration the limitations and opportunities around big data.

Beneficiaries

New data tools and technological advancement may empower individuals to directly intervene in human rights and security in new ways. But the democratization of human rights advocacy through

---

40 Intellectual Property and Human Rights, World Intellectual Property Organization & the Office of the United Nations High Commissioner for Human Rights (Nov. 9, 1998), http://www.wipo.int/edocs/pubdocs/en/intproperty/762/wipo_pub_762.pdf.

41 Erick Voeten, *Can forecasting conflict help to make better foreign policy decisions?* The Monkey Cage (July 28, 2013), http://themonkeycage.org/2013/07/28/32299/.

big data and technology can also generate new vulnerabilities. Citizens should balance their new ability to speak truth to power with their concerns about privacy and security.

Practitioners, technologists, and policymakers should keep beneficiaries' needs central in making determinations about data in the human rights and human security domains. Without their trust, many of the positive outcomes of these technologies will not be realized. This is particularly important in areas where technologies have been used for human rights abuses. Decision makers should adopt clear and carefully considered policies regarding consent, data ownership, and security. Technologists and human rights practitioners may need to develop new tools to allow citizens to safely share information relevant to human rights while protecting their identities. Where data allows for the individual identification of victims of abuse, they should develop protocols for communication and intervention that consider individuals' privacy and dignity. Bringing direct beneficiaries to the table when data policies and technologies are being discussed can mitigate harm in local contexts.

Next Steps

The human rights, human security, and technology sectors are remarkably dynamic. As new data techniques and tools emerge, specialists in these fields must ask which technologies have the potential to bolster their work, and what opportunities and risks they pose to vulnerable populations. While most of the challenges and opportunities discussed above apply to a broad range of technologies, delving more deeply into specific case studies of data on human rights and human security can highlight the actual benefits and risks. Examples of case studies range from data mining to combat human trafficking,[42] mobile data and unsafe migration, unmanned aerial vehicles and political violence, human rights and cyber-warfare, and private sector data sharing.[43] In addition, more work needs to be done on beneficiaries, including the disparate impact on "users at risk," which includes minority groups, dissidents, and journalists.[44]

Developing a strategic path forward includes field building, conceptual work, mapping, stakeholder analyses, case studies, workshops, education, multisector convenings, policy briefings, and cutting

42 *Technology and Human Trafficking Initiative*, USC Annenberg Center on Communication Leadership & Policy, https://technologyandtrafficking.usc.edu/.

43 *Responsible Data Forum on Private Sector Data Sharing-Event Summary*, United Nations Global Pulse (Aug. 25, 2014), http://www.unglobalpulse.org/RDF-private-sector-data-summary. *See also*, *The Data Collaboratives: Exchanging Data to Improve People's Lives*, NYU GovLab, http://thegovlab.org/datacollaboratives/.

44 Deji Olukotun, personal communication, June 17, 2015.

edge research and development. Through these efforts, guidelines and guiding principles can be developed for multiple stakeholders in different contexts. While some of the issues raised in this primer can be resolved, others will remain as important social, political, and technical challenges.

Data & Society is a research institute in New York City that is focused on social, cultural, and ethical issues arising from data-centric technological development. To provide frameworks that can help address emergent tensions, D&S is committed to identifying issues at the intersection of technology and society, providing research that can ground public debates, and building a network of researchers and practitioners that can offer insight and direction. To advance public understanding of the issues, D&S brings together diverse constituencies, hosts events, conducts directed research, creates policy frameworks, and builds demonstration projects that grapple with the challenges and opportunities of a data-saturated world.

For more on Data & Society's **Program on Data, Human Rights, & Human Security** see http://www.datasociety.net/initiatives/additional-projects/data-human-rights/.

Acknowledgments

Laura Seago made important contributions to this primer. Alex Rosenblat, Alexandra Mateescu, Angie Waller, and Seth Young provided key assistance and the fellows, staff, and leadership and Data & Society gave invaluable feedback. Jos Berens, Theresa Harris, Deji Olukotun, Kristin Antin, Danna Ingleton, Keith Hiatt, and Corrine Cath graciously reviewed early drafts of this work.

Contact

Dr. Mark Latonero
mark@datasociety.net
Data & Society Research Institute
36 West 20th Street, 11th Floor New York, NY 10011
Tel. 646-832-2038
www.datasociety.net