Strengthening Human Rights Worldwide

Exploring the Viability of a Human Rights Technology Research and Development Lab

Table of Contents

Introduction

In November 2014, Ford Foundation and Global Human Rights Program Officer Louis Bickford approved a grant in support of a project proposal submitted by Aspiration, entitled *Strengthening Human Rights Worldwide.*

One of the grant activities was an investigation and assessment of the advisability and viability of a "Research and Development Lab for Human Rights Technology".

This report summarizes the research and corresponding findings of , and is structured into the following sections:

- Research Overview
- Research Findings
- Conclusions
- Appendix

Research Overview

Our research into the viability of a Research and Development (R&D) Lab for Human Rights Technology was structured around consultations with a range of stakeholders from across the human rights technology sector. We sought to balance disciplines, roles, and geographies in our engagement and discussions.

The study focused on whether there is both a need and a role for an R&D Lab that seeks to anticipate digital needs and digital threats on the road ahead, while also prototyping and developing appropriate solutions to address those needs and threats.

To the extent that such a need and role for a future-focused Lab was affirmed, the study also attempted to paint an initial picture of how such a venture could be chartered and instantiated.

Context and Goals

Over a decade of work across the human rights technology sector has provided Aspiration opportunity to observe a diversity of factors and shifts that have shaped the state of the field today.

Over that time, we have seen one dynamic recur consistently. A substantial majority of human rights technology efforts, whether responding to an incident and mitigating a specific threat, or working on technology features and usability, or doing evaluation and risk assessment, seem to be reactive and short-term in nature.

This motivated us to consider how stakeholders in the sector might move to more proactive approaches to technology planning and preparation.

One direction that such an effort could take was that of a Research and Development Lab for Human Rights Technology. We selected this concept as a lens through which to explore what type of initiative might create new space and opportunities for stakeholders across the field to strengthen digital security capacity and operate more sustainably in their ongoing programmatic work.

Research Objective

We invited a diverse set of stakeholders to share their reflections on the advisability and viability of Research and Development Lab for Human Rights Technology.

Such venture was described as aiming to:

- Model potential future threats and adversaries and their capabilities;
- Anticipate tool, process and capacity needs NGOs and other human rights stakeholders will face;
- Model how actions we take in the present and near-term may eventually have adverse or unanticipated consequences.

Our investigation worked towards envisioning the foundation of an innovation center operating from a long-term standpoint, with a proactive approach to technology and scenario modeling. Through interviews conducted as part of the research we also aimed to gather reflections and feedback on the possible forms and focus areas such a Lab might take on.

Research Design

In order to gather a diverse range of perspectives, we engaged different types of professionals working across the human rights technology sector.

The types of stakeholders we consulted with included:

- NGO staff members;

- Software developers and technologists;

- Researchers;

- Funders.

Due to the limited resources and time available to conduct the research, we were not able to include a wider and more demographically and geographically diverse network of interviewees in our survey. In particular, representation of Global South perspectives is below the goals we set in our outreach.

This research does not aim to be a comprehensive investigation and it presents the pool of practitioners as a representative sampling. However, we believe the insights gathered could be useful to many interested in starting a cross-network conversation about the opportunities lying ahead for the human rights technology sector.

Research Findings

This high-level summary of the research findings is organized as followings:

- **Exploring present efforts and approaches focusing on a long-term horizon**. This section includes:

  ◦ Reflections on the meaning of a long-term effort in the human rights technology space;

  ◦ Thoughts on long-term approaches currently present in the field;

  ◦ Questions to address regarding the future state of play;

  ◦ Considerations about actions that could help anticipate future contexts.

- **Evaluating the viability of a Human Rights Technology Research and Development Lab**. This section focuses on:

  ◦ Reflections and questions on the viability of the project;

  ◦ More specific considerations about the project's framework, divided into:

    ▪ Guiding and foundational principles;

    ▪ Strategic focus;

    ▪ Programmatic design principles;

    ▪ Governance and operations;

    ▪ Ongoing learnings and dissemination of findings;

    ▪ Possible impact scenarios;

    ▪ Specific technology research areas;

    ▪ Unresolved questions.

Establishing the horizon of a long-term effort

Opinions about the suitability of a 10-year horizon as a time frame in which to think about future human rights technology scenarios were well-distributed across a spectrum of opinions.

Reflections in favor of a 10-year time frame

Interviewees advocating in favor of a 10-year time frame for modeling future human rights technology developments highlighted a range of motivations for their position.

A 10-year period was considered necessary to allow the analysis of the contexts in which technology operates, and to understand how to employ it as a tool to contribute to social change. This approach invites one to think about the human rights technology ecosystem as a movement, with a potential for long-term strategy which, similarly to how social change organizations function, is built looking decades ahead in the future.

The 10-year time frame was also seen as a fair period to allow planning for long-term infrastructural challenges, required by policy, technical or capacity building needs among others. This thinking also underscores the need for associated funding cycles to be structured on a longer-term basis, as opposed to the more prevalent short-horizon, near-term return on investment (ROI) models of support.

As outlined by one interviewee: "My impression is that organizations tend to think on the scale of the funding cycle (2-3 years) or even less, depending on if they are reacting to policy changes, technical needs, or capacity building needs. This means civil society is placed in a vulnerable position that doesn't really allow to plan for long-term infrastructural challenges".

Ultimately, there are research and development areas within the human rights technology space which specifically require a decade-long outlook, due to the pace at which they evolve. A few examples mentioned: efforts relating to industries which have not yet engaged with human rights issues but which are essential actors to pressure, such as the hardware industry or first level telecommunications companies; research focusing on elliptic curve cryptography.

In general, those in favor of the longer time frame felt it would push thought boundaries by inviting practitioners of all types to think outside of present comfort zones and beyond the great majority of horizons being modeled in various projects and pursuits.

Reflections in favor of a time frame shorter than 10 years

Interviewees less inclined to embrace the 10-year frame expressed their views in relation to the pace at which societal, political, legislative and technological scenarios change globally. Increasing rates of change influence the emergence of new threats and needs, and correspondingly impact work within the human rights technology space.

As mentioned by one interviewee, "Technology-wise, a 3-5-year frame is now the equivalent of a 10-year frame of the past. Most countries in the world have presidential cycles of 4 years and this substantially changes the shape of societies globally. All this considered, a 5-year frame should be a suitable measure to think about our field".

Another interviewee pointed out that also "the way technology has come to be developed and distributed plays in favor of adopting a time frame shorter than 10 years". Today tools are developed, deployed, tested, released and updated at a way faster pace than ever before.

To this, the interviewee adds a critical point: "In addition to this, we need to look at the legal climate: how fast that changes, and how it affects the technology solutions we design to serve different contexts under different legislations".

Looking at the risks that human rights defenders face, this group of interviewees saw a 3-5 year horizon as a more useful time frame in which to situate research on human rights technology.

It was also emphasized that a certain level of flexibility is essential when it comes to estimating time frames in this context, since the risks faced by human rights organizations are a consequence of how scenarios and threats develop, and of how quickly adversaries improve their tactics. All of these elements are complex to predict.

Moreover, the work done by media and advocacy organizations in regard to reporting the challenges faced by human rights defenders was mentioned as one of the elements to consider in favor of a shorter time frame.

As observed by one interviewee: "Human rights and technology are vast fields, formed by many different aspects: anticipate their developments on the long term is very challenging. Observing the landscape in which they intersect, it is key to consider the influence that media outlets and advocacy groups can have, ultimately contributing to shape the future developments of the scenarios they get involved with. Just think about how drastically the awareness around human rights technology has changed in the past three years, since the NSA revelations of 2013. What the civil society knows today about it was imaginable just a few years ago".

Reflections in favor of a time frame longer than 10 years

One interviewee pointed out that considering a 10 to 20-year time frame could be very helpful to research and model for future stages of internet architecture, a key component at the core of the work of human rights organizations and defenders worldwide.

This research angle would allow to model and articulate the technical principles aiming to ensure that the internet continues to grow and evolve as a platform for global communication and innovation.

As said during the interview: "A time frame of 10-20 years would be helpful to build a new and much needed involvement of civil society in the decisions about internet infrastructure, now taken at tables exclusively reserved to telecommunications companies. Our strategizing and operating in internet governance should become much more adult and based on research and knowledge […] Also, brilliant research is already done in academia, but because of how academia is modeled, this work is not openly and collaboratively shared. A time frame of 10-20 years could also allow us to try to connect with scholars with profound understanding of technology and social science, and integrate their knowledge in our work".

Bridging between time horizons

Interviewees also surfaced the possibility of combining a flexible 5-year look-ahead for technology-related needs with the more traditional 10-year-horizon approach employed by human rights and social change organizations. This composite model would integrate the positive aspects of short-term technology development iteration together with a long-term strategic approach to infrastructural and societal challenges.

Reflections shared by one interviewee nicely summarize this thinking.

"I think about human rights organizations that have been successfully around for decades, and this makes me realize that we can think in terms of decades when it comes to efforts in the field. When it comes to human rights technology, I think we should move out of the 'pipeline and production schedule' approach of Silicon Valley and take cues from how human rights NGOs think in terms of multi-year or 10-year time frames. This does not necessarily mean abandoning the positive aspects of short-term technological iteration that we learned to work with in the past few years. Thinking about technology in a disposable way, being open to fast prototyping, testing and failure has solid value. So let's combine the best of a long- and a short-term approach: we can keep the positive aspects of iteration, and combine them with the thoughtful and strategic long term approach traditionally taken by human rights and social change organizations".

Working within a hybrid time frame could also allow implementors to simultaneously dedicate resources to fields that are equally critical, but operate at different paces: flexible technology development in service of fast-evolving user needs, and technology capacity building efforts with a long-term outlook.

As one interviewee pointed out: "An R&D Lab should equally focus on proactively and promptly address the technical needs of human rights organizations, and develop educational methodologies with a long-horizon outlook designed for them. Technology capacity building allows building participatory learning opportunities with and for human rights defenders, and is fundamental to support their work. Technology capacity building contributes to create digital literacy. Digital literacy is not about being trained to use a specific tool: it is the ability to critically assess any digital tool. Ultimately, without technology capacity building, any tool loses much of its potential to help".

Current long-term approaches in the field

A number of approaches were referenced as positive examples within the field of long-term outlooks on human rights technology. Examples span different stakeholders operating across the ecosystem, from users to the producers, deployers and funders of said technologies.

- Human rights organizations investing in their security culture taking a holistic approach which simultaneously focuses on their physical, psycho-social and digital security.
- Trainers focusing on holistic information security with the aim of helping human rights organizations strengthen their long-term capacity.

- Advocacy organizations building awareness about digital rights and information security, helping human rights organizations and civil society alike to prepare for future contexts, needs and threats, and encouraging a meaningful shift in security culture.

- Researchers bridging the communications gap between information security specialists and human rights defenders.

- Technology creators prioritizing usability, accessibility and adoption of their tools from the beginning of development cycles.

- Funders investing resources in long term efforts, specifically regarding:

  ◦ Technology development, investing in and incentivizing the growth of a network of technologists focused on cooperating on complementary and collaborative efforts;

  ◦ Technology capacity building, for the organizations and networks they support as well as for themselves;

  ◦ Projects with regional focus, providing necessary funds to do context-specific research where results can benefit the work of the field as a whole.

Questions to address regarding the future state of play

Regardless of the forward time horizon in play, interviewees highlighted topics and questions that they considered to be critical for a robust look at future scenarios of human rights technology in the context of a potential R&D Lab.

Equitable decision making

Across the breadth of the human rights technology field, large questions remain on how to ensure that voices from the Global South and marginalized communities are empowered stakeholders in discussions and thinking aimed at modeling future states of play. How can we make sure that decisions with global influence and consequences do not continue to be driven by Northern perspectives?

Internet infrastructure

Which networks will constitute the future internet backbone, and who will own them? Modeling the internet infrastructure of the future and safeguarding its accessibility are among the critical actions necessary to protect digital and human rights rights globally in years to come.

Particular concerns were raised in relation to the development of 5th generation mobile networks (5G): "5G is a closed platform controlled by telecommunications companies. It is possible it will replace wired networks, replacing IP, becoming the bottom of the stack. This would mean going back to being owned by telcos. I see this as a very stifling scenario".

Internet governance

How will the ever-expanding internet be governed in the future? How do the rights and decisional power of civil society, governments, and private sector intersect with its governance?

It is crucial for human rights technology stakeholders to be involved with the creation and development of the principles, norms and decision-making procedures that will influence the way the future internet will be designed, used and managed.

This becomes all the more true as billions of "Internet of Things", "smart car" and "smart building" devices come online, increasing dependence on internet infrastructure in more facets of our collective lives, while simultaneously making surveillance capabilities more ubiquitous and attack vectors more plentiful.

Access to secure technology

Human rights technology need access to secure technology, but current scenarios worldwide are far from what would be ideal. Telecommunications services, internet providers, data storage products are all central elements of the work of NGOs, and too often the most accessible and usable solutions on the market are not the most secure.

It is therefore critical to focus on modeling how to improve human rights organizations' and defenders' access to secure technology. Such analysis requires tackling multiple levels of challenges: technical, political, and economical.

From a technical standpoint, in order to address users' needs, secure technology needs be designed within a framework which pays attention to accessibility, usability, localization, through thoughtful user research, testing and feedback loop processes.

An increasing number of cases worldwide demonstrate how the use of an encrypted or anonymous tool can be a sufficient reason for a user to be seen as engaged in suspicious activities, and as such monitored, harassed or persecuted. Therefore, the development of secure technology needs to coexist within a solid understanding of the political and legal context its users operate in.

Finally, researching and developing access paths to secure technology requires the acquisition of a solid understanding of how the corporate sector affects the access to secure technology. Today's global connectivity is dominated by a small number of powerful corporations controlling the tools which millions of people use to communicate, connect to the internet, and create, store and share their data. We know today that the corporate sector has often handled its power to benefit the interests of inner circles and key investors over their users', in some cases also endangering their digital and human rights.

As observed by one interviewee: "We need to look at the access challenges of secure technology from new perspectives. They occur in a context of late stage capitalism, and we should investigate the problem starting with an analysis of capital".

Human rights organizations needs

Human rights technology within organizations needs to be founded on a very intentional user centric approach, and addressing the questions posed by any future states of play demands a close look at the needs of human rights organizations.

In this regard, the interviewees highlighted the following focus areas.

- **Data protection**

  As outlined by one interviewee: "Human rights organizations still don't have a system or tool that allows them to share, store, access, sort information easily and securely. Especially when legislators are censoring and policing the activist community, getting information out safely and timely is essential". Data is an organization's power. The ability to be in control of their data, from the moment it is produced to when it is communicated, shared and stored is of fundamental importance to efficacy, independence and security.

- **Technology capacity building**

  Human rights organizations require digital literacy which suits their needs, contexts and resources. Tool-centric trainings can not fully address this need. What can help is a thorough technology capacity building protocol, guiding organizations to assess their needs, identify their assets, learn how to make technology decisions based on their

requirements, independently from how tools and the technology market change over time.

- **Sustainability**

    Several interviewees highlighted the need for more thorough reflections on the role that technology will play into the work of human rights organizations in the long run, specifically in regard to their sustainability.

    As observed by one interviewee: "How will technology impact the long term sustainability of human rights organizations? How will it contribute to their survival? To answer these questions, I think we need to analyze two aspects. First, the technical infrastructure they find themselves working in: their context. Second, the technical infrastructure directly helping them in their work: the tools and processes they can use and engage with".

Technology development

The development of technology solutions in service to human rights efforts exists at the intersection of power dynamics, technical challenges, legal and political contexts.

The complexity of this landscape surfaced during the interviews, conveying how different actors and settings can affect the development of human rights technology. Complex issues to be considered as technology is prototyped include:

- **Adversaries**

    Technologists focusing on helping human rights organizations can often feel frustrated, as their efforts to proactively anticipate their users' needs often get neutralized by the increasingly fast-evolving sophistication of their adversaries' technologies. One interviewee posed the question: "Will technology be the means to to solve this power imbalance?"

- **Data protection and access policy**

    Technology is increasingly present in societies worldwide, and in some regions, as a consequence of greater internet access, this ubiquity is evolving at a particularly fast pace. This in turn allows practitioners to observe how policy and the public discourse react to such rapid technological change, and how data protection and access are discussed and handled in these contexts. Can an analysis of this landscape help us model for future technological policy debates?

    As outlined by one interviewee: "We can learn a lot from the current conversations over privacy and data in US, Brazil, EU and many other countries and anticipate similar challenges for what is commonly refereed to as the next billion Internet users. I think the foremost broad question should be how can we turn today's challenges and lessons learned into opportunities. Because as these technologies reach users in different countries, they will undoubtedly be both effected by our current decisions over data protection and access, and will also face similar challenges over privacy".

- **Funded coordination of efforts**

   The network of technology projects aiming to serve the needs of human rights organizations is steadily growing. But, as observed by several interviewees, the efforts of different projects sometime seem to be conducted disjointedly, missing the opportunity to maximize their impact acting as a community with a shared objective.

   Aiming to shift towards a more impactful state requires to unfold two challenges: strategic coordination and funding.

   "The community of organizations working on human rights technology should coordinate its efforts. To do so, it should try to operate like a company, with one single goal. How the organizations get to it is their business, but they have that one goal they all agreed on, and they are all going in the same direction.

   I think that many organizations would already like to do so. But funding for this space is limited. Technical projects end up having to compete to get the funds to be able to work, and cannot invest in cooperation when they are risking to close down. So what would also be much needed, would be funders understanding the importance of cross-network coordination, providing financial resources to operate with this model".

Funding

Funding is of critical importance to support both innovation and sustainability across the human rights technology space.

When it comes to modeling for future states of play, foundations need to focus simultaneously on gathering learnings from past and current issues encountered and anticipating potential future opportunities across the field. The complexity of this challenge was addressed during several interviews, and the following are the questions which seem to emerge ubiquitously.

- How to structure the funding directed to human rights technology in a way that enables coordination over competition between the organizations working across the field?

- How can foundations best gather an understanding of actors and dynamics playing across the human rights technology ecosystem, to operate in the space with increasing efficacy and model for its success on the long-term?

- What funding models could most effectively and strategically support the human rights technology community in becoming increasingly sustainable?

Corporate engagement

From a capital perspective, we have gone from a competitive market to a market that is now divided between a very few big technology companies controlling fundamental services like telecommunications and internet access.

This scenario deeply affects the work of human rights organizations, and engaging with the corporate sector has become a necessity for the human rights technology sector.

The protection of data, and a user-centric revision of terms of services and privacy policies need to be prioritized by the corporate sector.

Furthermore, the need for stronger cooperation between social media companies and the human rights sector is increasingly critical to address the complexity of digital rapid response protocols.

The dialog between the corporate and the human rights sector is still unsteady, and much stronger ties should be developed to allow for coordination, and hopefully work toward revising damaging policies and monitoring the impact of changes over time.

But how can organizations advocating for digital rights engage with companies? And is advocacy all that is needed to establish a fruitful dialogue?

Specific areas of concern

The following list is not meant to be a comprehensive overview of current areas of concern in the human rights technology field. It is a list of themes that emerged during the interviews and is included in this report due to its relevance to the research.

- **Predictive analytics**

  From predictive policing to the social media tracking of individuals deemed to be a potential threats for a state's national security, governments worldwide are increasingly relying on data-driven risk assessments. But predictive technology comes with risks. Feeding unrepresentative or biased data into predictive algorithms can lead to incorrect answers which can bring unjust harassment and prosecution of individuals and groups and violation of their rights. Moreover, predictive technology is still rarely accountable to the civil society and in several countries its adoption often precedes the existence of policies regulating its use.

- **Biometric technology**

  Biometric technology is increasingly used to recognize or verify the identity of individuals in public and commercial spaces as also employed as a method of border control. This practice has a multitude of human rights implications regarding the collection, processing and distribution of individuals' identifiers, and has been raising concerned reactions worldwide. Human rights organizations have reported several cases in which this methodology has resulted in discriminatory application and effects. A thorough opposition to its unaccounted adoption is now deemed as critical across the entire human rights technology field.

- **Artificial intelligence**

  Artificial intelligence (AI) and machine learning technologies are steadily being developed and prototyped, and their field of play is so vast that they will certainly present a wide swath of opportunities and challenges for the human rights sector.

  In terms of challenges, accountability and ethics are of fundamental concern across the human rights sector.

The unaccounted adoption of AI technologies will have the potential to exacerbate forms of inequality and discrimination. Even more dramatically, as outlined by a 2015 [report by Amnesty International](#)[1] on these matters, AI is among the advancing technologies that will make possible the development of fully autonomous weapons systems able to operate without effective human control.

If the human rights technology community does not promote the establishment of values-based standards for the AI industry, then the biases of its manufacturers will define AI's consequences for humanity.

It is therefore critical to create a transparent dialogue between stakeholders to prioritize the creation of ethical standards for AI technologies, advocate for a human rights observing regulation of their employment, and leverage the innovation they could bring in support of human rights efforts.

- **Social science**

The analysis of the intersections between human rights technology and social science would greatly benefit and strengthen the field, providing a more comprehensive picture of the scenarios human rights organizations currently operate in as well as key knowledge to inform the sector's proactive and long-term efforts.

As stated by one interviewee: "Any functional long term R&D Lab should not only focus on technology. It should also focus on sociology, political science, economics, human geography, demography in order to be able to envision future states of play though the analysis of power dynamics. This would create a real innovation space, way more effectively than a new app or a new tool could ever do. Such a multidisciplinary approach would be about creating a new influence and support for the human rights community as a whole".

- **Gender- and sexual-based online violence**

Organizations focusing their efforts on the protection of women's and LGBTQIA rights face very specific challenges when using technology in their work. Gender- and sexual-based discrimination ingrained in social, cultural and religious constructs results with alarming frequency in online violence, ultimately limiting the organizations' freedom of expression, right to free and full participation and right to safety and privacy.

Addressing this extremely complex issue requires the concerted efforts of a multitude of stakeholders. Governments and corporations need to formalize policies based on the harm experienced by the targeted groups; corporation and human rights technologists and advocates need to coordinate and develop better workflows to report and respond to online violence; security trainers need to create spaces and resources specifically dedicated to counseling and training women's and LGBTQIA rights defenders.

1https://www.amnesty.org/en/documents/act30/1401/2015/en/

Actions that can help anticipate future contexts

What does a proactive approach to human rights technology look like in practice? The following is an overview of the steps that, in the interviewees' opinions, different stakeholders across the space could or should take to anticipate future challenges and scenarios.

Internet infrastructure and governance

Decisions about the future infrastructure and governance of the internet cannot be left to telecommunications companies. Stakeholders across the human rights technology field, especially those with strong knowledge of technical infrastructure and social science governance structures, should enter decision-making spaces. Strategizing and operating in internet governance should be based on research and knowledge, and become a priority.

A regional approach to internet policy

Over the last decade, digital technology and the internet have increasingly and progressively influenced societies worldwide. Public authorities on the national and international level have started to respond to the political challenges presented by this ever-changing scenario, thus engendering the internet policy field.

While operating within the global framework of the internet infrastructure, the internet policy field has been increasingly coordinated and implemented by national or regional authorities, in an attempt to regulate issues such as data protection, security and access more closely to the socio-political context where they take effect.

As a consequence, the development of human rights technology needs to be informed by a context-specific knowledge of the internet policy landscape within which it would be used.

It is within this premise that one interviewee says: "Internet policy and technology need to be investigated at the same time as they are deployed".

Another interviewee points out: "Technology, such as in the form of apps will cross borders, but internet policy is becoming more regional. […] [It is necessary to understand] how these technologies, their data protection policies, privacy policies can be potentially abused and harmful to human rights and civil society in countries that do not offer some of the protections provided by different legal systems and to pressure companies to formulate and act on policies that ensure safeguards against such abuses".

Information security and data protection

Everyone has the right to the protection of personal data. And stakeholders across the human rights technology field, from human rights organizations to researchers and funders, can already exercise this right with the means at their disposal, using free and open source technology and taking a holistic approach to build the security culture that best fits their needs, context and resources.

Measures such as acquiring knowledge about the importance and achievability of effective security practices, preferring locally managed services over cloud-based solutions, regularly

inventorying and backing up information, and using secure communications channels, can dramatically help to improve the security of their operations, their staff, and the targeted communities and individuals they work with and for.

Usability and accessibility

No users can be secure if the secure tools designed for them are not accessible and are ultimately not adopted. User experience design is an essential element for the creation and improvement of secure technology. Organizations building new tools need to:

- Conduct user need assessments;
- Coordinate the collaborative work of software developers together with graphic, visual and interaction designers;
- Test their tools and be responsive to their users' feedback.

Participatory technology development process

Participatory methodologies can be of critical importance for the development of user-centered technologies and can ultimately facilitate the achievement of truly meaningful outcomes and impact. The intentional involvement and participation of users from the very first planning stage of a tool to the testing, prototyping and deployment phases should become a regular practice across the field.

As pointed out by one interviewee, "Too often, technology projects are developed in a boardroom and then tested out with their users only at a later stage. This is a very patriarchal management, it is abuse of power. Human rights technology has to: be very responsive to societal dynamics; make sure it does not disrupt the already fragile power dynamics of the contexts where their users live".

Secure tools for migrating communities

Projected trends of the next 5 years indicate that an increasingly high percentage of the global population will be migrating, due to factors that include climate change and regional strife.

As one interviewee said, "We need to build and fund technology solutions for people who do not have stability, who do not have access to power all the time, nor have mobile internet, who can only use cheap devices, and are subjected to digital as well as physical threats".

And consequently, as further outlined by the interviewee: "If the technology we build will work for this persona, users who are in less challenging situations will also be served and secure".

Stronger ties between technologists and legal scholars

Knowledge of the legal scenario where a tool is deployed and expected to be used is key for the technologists working on the development of technologies aimed at supporting human rights efforts.

Likewise, technical understanding is of critical importance for legal scholars working to protect and reclaim human rights observing policies, when these intersect with the digital and technical realms.

One interviewee stated "There is a strong need for cooperation between technologists and legal scholars. Knowledge sharing between them would help to understand."

Hardware security

The development of more secure and trustworthy devices is an essential component of the future of human rights technology. An increasing number of projects and academic researches are focusing their attention on secure hardware, but interviewees pointed out that this field of work still needs much support.

More specifically:

- Spaces designed for professionals focusing on hardware security to connect and collaborate on common projects would contribute to advance the sector and grow the network around it;

- Advocacy organizations could greatly help the sector by engaging hardware companies on human rights and operational security matters;

- Funds dedicated to hardware security projects would be necessary to support the research and development in the field, deemed by a number of interviewees as currently lacking the financial support that would allow it to advance relevantly.

The future of information security training

Information security training and the acquisition of a solid security culture are essential to the work and sustainability of human rights organizations. The training field is constantly developing, and technology capacity builders are progressively making their work known with participatory, holistic and long-term approaches to education.

The knowledge at the core of the technology capacity building community is already mature, and an increasing number of human rights organizations around the world are benefiting from delivery of that knowledge. But the NGOs in need of support outnumber the tech capacity builders operating in the field, and practitioners working in this space agree that many aspects of their work would benefit from improvements that will allow them to further professionalize their area of work and expertise.

As one interviewee underlines, the needs are numerous. Among the most pressing ones:

- "Becoming known as a learning-entity, as opposed to an install-and-configure-entity", as digital literacy is not about being trained to use a tool, but about acquiring the ability to critically assess any digital tool;

- Collaborating to improve training methodologies;

- Creating a support system to handle all financial aspects of the profession, from compensation levels to pension plans;

- Coordinating across the sector to help making it grow.

Technology intermediary organizations

Technology intermediary organizations can help to bridge the gaps between the stakeholders operating in the human rights technology field, ultimately facilitating the connections between the supply and demand sides of the ecosystem.

But they are not nearly large enough in number to address the needs of the human rights sector. As agreed by numerous interviewees, they would greatly benefit from dedicated resources to support the growth of a stronger, wider and sustainable global network of intermediary organizations.

In the words of one interviewee, "There is a strong need to diversify and increase the number of technology intermediary organizations, because now they are too small, and too few. Wide geographical support is needed, and there should be enough intermediaries to offer support at both regional and local level. Developing such field/network is the responsibility of both funders (providing resources) and existing intermediaries (designing how to build such network), together".

A new language to talk about technology

Simply thinking that staff members at human rights organizations would need more technical knowledge has not proved to be a successful model to help NGOs and activists with the information security needs.

As one interviewee recommends: "It is necessary to find a new language to talk about technology, more accessible, approachable, and open to different skill sets".

When focusing on a holistic approach, technology intermediaries and trainers can make a tremendous difference with their work, helping to bridge the gap between technologists and human rights organizations.

Moreover, with a new language comes also the opportunity to create a new technology culture: user-centered, inclusive and receptive to the needs of different cultural, societal and political contexts.

Approaches to funding

During the course of the interviews, some recommendations regarding new approaches to funding were shared.

The following is a recommendation made to funding entities:

Funders who have strong ties to other stakeholders across the field, who listen to and learn from the needs and challenges faced by the community, should share knowledge and awareness, and particularly with regard to their own sources of funding.

The following is a recommendation to funded stakeholders:

Human rights organizations, technology builders, trainers, intermediaries, researchers work in a very competitive environment, chasing the same funding sources to be able to sustain their

work. Not only is this a distraction from the actual work, but, at the point when multiple organizations focused on the same problem compete for the same funds, it also turns into counterproductive redundancy. As mentioned by two interviewees, it would be interesting to revamp this model, from competitive to collaborative.

Evaluating the viability of a Human Rights Technology Research and Development Lab

Reflections and Questions on the Viability of the Project

The foregoing sections lay out the potential mandate and scope of activities any forward-looking research and development undertaking. What follows is analysis on the viability of an entity that might carry out some form of this mandate.

We outlined the conceptual idea of a "long-term Human Rights Technology Research and Development Lab" to the interviewees participating in the research.

The project was described as a hypothetical effort with a long-term outlook, focusing on modeling future scenarios, providing recommendations, prototype tools and approaches designed to proactively and sustainably support the work of different stakeholders across the sector over time.

The majority of the interviewees expressed positive feedback about the general concept.

The idea of a long-term effort was seen as a needed complement to the many short-term efforts currently active in the space.

What the majority of the interviewees were interested in were two specific aspects of this type of concept:

1. The opportunity to create a space for interdisciplinary work on human rights technology, facilitating the connection of organizations and practitioners with different skill sets to collaborate on common projects;

2. The chance to structure this type of effort as a meaningfully human-centered, network-driven, analytical and holistic project. This would translate into:

   ◦ Reflecting the demographics it aims to serve in the appointment of its founding and executive members;

   ◦ Scouting and leveraging the most valuable work done across the human rights technology network, as well as facilitating participatory collaborations;

   ◦ Conducting ongoing analysis of societal, political and legislative contexts, from the global to the regional level, to solidly inform its mission, ethics, and approach;

   ◦ Working on tools and processes to always serve the most endangered persona of the case in point first;

   ◦ Grounding its work, recommendations and intervention in a holistic, long-horizon, and sustainable perspective.

Considerations on the Project's Framework

While discussing the viability of a Human Rights Technology Research and Development Lab, interviewees shared thoughts about how they would envision the project if it were to become reality.

The following is a catalog of their considerations in this regard, sorted by theme.

Guiding and foundational principles

Any Research and Development Lab to be initiated should be founded on acknowledged key values. Those should be at the basis of every endeavor undertaken by the institution.

The following are the guiding principles emphasized during the course of our interview series.

- **The Lab would wholly operate in service of human rights efforts.**

  The Lab would exclusively research and develop technology helping to build power in organizations and movements working to reclaim and protect human rights and achieve social justice. Any other purpose would defeat its objective and should not be pursued.

- **The adoption of technology to solve an issue is not a default choice, and should always be thoroughly motivated by the users' needs.**

  No technologies should be developed until the workflows they support have been described, stakeholders in those workflows have verified the accuracy of such workflows and affirmed that the technology plan supports the way they operate, rather than defining the same.

- **Any endeavor undertaken by the lab should be user-centered.**

  User needs should be the primary reason why research and development would be conducted, and user experience and user interface design should be at the core of every technology development effort.

- **The research and development outputs produced by the Lab should be open knowledge and open data.**

  The results of its work should be free to use, re-use and redistribute. Doing so, the lab would contribute to further analysis and developments across the field, provide resources in support of capacity building efforts, and consolidate understanding and literacy about human rights technology.

- **The technology developed by the lab should be free and open source.**

  Open source technology solutions allow human rights organizations to be in control of their own operations and processes. In fact, open source software it is more accountable, transparent and reliable than closed and proprietary software since it can be openly tested, reviewed, also fixed. Consequently, and fittingly with the aims of an R&D Lab, open source development offers the potential for a more flexible technology and quicker innovation.

- **Research should be followed by development.**

The aim of each research endeavor would be to reach a development phase. Research outputs would be used to iteratively prototype, deploy and test tools and processes with their users.

Strategic focus

The core purpose of the Research and Development Lab would be to strengthen the work of human rights organizations in the long term.

To elaborate, the following are objectives to which interviewees drew attention:

- **Support and facilitate the formation and growth of a diverse network of researchers, technologists, intermediaries, scholars supporting the work of human rights organizations.**

  The Lab would focus on serving and strengthening the community, by facilitating connections and collaborations, promoting its sustainability and contributing to making it thrive on the long term.

- **Model how actions we take in the present and near-term may have adverse or unanticipated consequences on the long term.**

  This would increase critical awareness about the current state of play, threats and compromises faced by human rights organizations. It would also contribute to giving human rights organizations fuller control of the operations and processes which are at the core of their work.

- **Model potential future threats and adversaries and their capabilities.**

  This would allow to gather the knowledge and data needed to update or create information security guidelines, resources and trainings.

- **Strategically center work around data, not technology.**

  Data is an organization's digital power. Software and hardware solutions will change overtime, but data will always outlive them. For this reason, an effort aimed at supporting the work of human rights organizations should first and foremost focus on the security, integrity, accessibility and portability of organizational data and not on the applications and platforms used to edit or store them.

- **Anticipate the needs that human rights organizations will likely encounter in the future.**

  The Lab should also concentrate its research on foreseeing the tool, process and capacity needs NGOs and other human rights stakeholders will face, thus informing the development of solutions aimed at addressing them proactively.

- **Provide recommendations and prototype, deploy and test tools to prepare for future states of play.**

  Such fundamental focus on iterative development with a long-horizon outlook would provide the necessary data for the Lab and human rights technology suppliers to better

support and equip NGOs, and contribute meaningful knowledge strengthening further analysis and developments across the field.

Programmatic design principles

Establishing a Research and Development Lab would require the recognition of programmatic design principles. These would represent the foundational values guiding the project's creation and its further developments.

The following are the core premises discussed by the interviewees.

- **Global direction**

  The development of a new R&D Lab concept would offer the opportunity to approach its conception with a global and inclusive outlook from the very start.

  A concrete example of this intent would be to ensure that funding sources as well as executive management of the Lab would not be constituted by a majority of organizations and professionals based in the Global North. Furthermore, it would be essential to involve, at both the executive and board level, professionals representing the vast spectrum of competences and backgrounds that can best help to understand the systems that the Lab itself aims to bring justice to.

- **Development and testing**

  The human rights technology field is well acquainted with excellent research projects. But currently there are only a few and their work does not often have the opportunity to go beyond the production of reports and recommendations, published with the hope of paving the way to further investigation and much needed development.

  An R&D Lab effort should help address the need for both more research in the space and, even more critically, for resources and projects dedicated to prototyping, developing and testing solutions making the most of the most advanced findings reported.

- **Unique contribution**

  A look at the current state of play shows that the human rights space is already populated by organizations and projects focusing on elements which could be read as part of what an R&D Lab would do. For this reason, numerous interviewees think it would not be advisable to create a new individual R&D Lab effort from scratch, as they think it would be redundant and it would miss the opportunity to build on the solid work done so far.

  What they find could be truly meaningful would be to frame a possibly upcoming R&D Lab as a facilitator. It would help build and strengthen the network of practitioners working on relevant aspects of research and development in the field, coordinate the collaboration of existing and new organizations and projects alike, and support the organized and open distribution of their outcomes.

- **Problem solving**

The R&D Lab should focus on reaching the most meaningful attainable solutions to address the needs of human rights organizations, even when these do not include the development of a tool or a platform. Results should be driven by a long-term outlook and aim to be sustainable, and sometimes outputs including capacity building, trainings, and new organizational practices could prove themselves to be much more helpful than a new app.

Technology should be considered as a tool that can help in addressing an organization's needs, but only if this has been proven for the case in point.

- **Working open**

    Working open is a key programmatic value to enable participation, flexibility, iteration and leverage. As such, it's a mindset that would greatly benefit an R&D Lab.

    It means working in public spaces, like shared documents and mailing lists, not to make a public performance of it, but to be transparent, accountable, and invite collaboration and ongoing peer review. It is a critical approach to building outcomes together as a community, making the most of the network's knowledge and enabling richer and faster iterations and developments.

    As pointed out by one interviewee, "The R&D Lab should be a space to learn how to work dynamically, iteratively building knowledge. Furthermore, by taking this approach, the Lab would also help human rights organizations to understand and learn how they can apply this methodology to their own work".

- **Openness to failure**

    As in any field, organizations and projects within the human rights technology space experience failure on a regular basis. Acknowledging this, and understanding the opportunity that learning from unsuccessful attempts provides to upcoming research and development, the R&D Lab should be open to taking risks and open to failure.

    This would allow the R&D Lab to work with more agility and flexibility, make the most of iterative collaboration and strengthen its development work through rapid deployment and testing, ultimately reinforcing its own effectiveness.

Governance and operations

According to the interviews conducted, requirements for any governance model underpinning the R&D Lab would be inclusivity, transparency, accountability.

- **Inclusivity**

    The governance model of the Lab should be as inclusive and community-driven as the work that it aims to produce. It should be a multi-stakeholder model, openly informing and involving its stakeholders, and ultimately leading to the creation of more resilient and adaptive operational systems.

    Such a model should particularly take into account the perspectives of groups and demographics that are often marginalized or in minority position in technology research

and development contexts, thus strengthening the genuine value of its work for the ecosystem it aims to serve.

- **Transparency**

    A transparent governance model makes information available to employees, stakeholders and the general public, and provides clarity about government rules, regulations, and decisions. Disclosure, clarity, and accuracy in both internal and external communications are key elements to achieving greater operational transparency.

    Transparent procedures include open meetings, open access to information, budgetary review, and audits.

- **Accountability**

    The governance model of the R&D Lab should be accountable to its stakeholders. It should provide reports about its operations and performance, answer concerns which might be raised in this regard, and be considered responsible and liable for its decisions and actions.

    Like transparency, accountability contributes to building and strengthening the democratic, open and trustworthy governance of an institution.

It is also worth noting that although the interviewees outlined the aforementioned requirements as key components of the R&D Lab governance, they also raised questions about the exact governance model that would be adopted to operate the Lab, thus suggesting the need for further research on different governance models were in fact such a venture to actually be established.

Ongoing learnings and dissemination of findings

In order to deepen and distribute knowledge across the field, the R&D Lab should create and maintain open learning streams.

The stakeholders interviewed provided suggestions aiming to address this demand.

- **Facilitating collaborative knowledge sharing opportunities between practitioners working in the human rights technology space with a long-horizon outlook.**

    By facilitating the creation of spaces dedicated to knowledge sharing between human rights organizations, technologists, and professionals working in the legal component of the space, the R&D Lab would greatly contribute to the consolidation of collaborative learnings as they evolve over time. Furthermore, by helping to create a framework to document and openly share said knowledge, the Lab would help the formation of an ever-growing collection of resources and recommendations supporting the work of stakeholders across the network.

- **Democratize digital forensics, supporting the creation and maintenance of a library of implementation stories.**

Such effort would aim to objectively evaluate past projects, identify learnings to build upon, and ultimately gather essential knowledge to prototype solutions addressing new, or still unmet, needs.

As pointed out by one interviewee, "We see excellent digital forensics work done in the field, often leading to very successful outcomes, from greater security for human rights activists to increased literacy, and media coverage of a case. These wins could happen way more frequently if we could democratize the process about how these postmortems happen. We could lift the curtain that separates ideal and on the ground implementation, and critically strengthen our knowledge and work".

- **Facilitating the creation of open repositories of digital threats and response methods**

  Such documentation and archival efforts would constitute a unique resource for stakeholders across the field, from technologists and researchers to end users. Examples of vulnerabilities deemed as particularly critical to be documented for the security of human rights organizations include malware attacks, communications interception, and internet network monitoring.

- **Conducting and publishing research aiming to model future states of internet infrastructure and governance**

  The outcomes of such research would equip digital rights and internet policy advocates with solid arguments to engage policy makers with evidence-based data. This effort would help them to advocate in favor of the internet as a free and open technology, and demonstrate how its infrastructure and governance can directly influence the protection of human rights globally. As mentioned by one interviewee, "There is the need to present a technology rationale to the people who do policy work, so that when they talk with governments they can better contribute to influence change".

Possible impact scenarios

The potential impact scenarios emerging from the R&D Lab's work could be numerous. The reflections shared by the practitioners interviewed for this research draw attention to some specific impact areas deemed to be of particular value for the human rights technology field.

- **Model future states of play for human rights organizations over the long term**

  The R&D Lab's focus on anticipating future challenges and opportunities in the field could greatly contribute to proactively supporting NGOs in their work. It would help to envision future needs and challenges faced by the organizations; foresee the adverse consequences that current practices and policies could produce; model potential future threats and vulnerabilities; prototype and develop solutions aiming to address all of the above.

- **Innovate threat modeling processes**

  By modeling potential future threats and adversaries and their capabilities, the R&D Lab would gather, and share, the knowledge necessary to innovate how threat modeling is applied, taught, learned, and implemented as a key element of work of all the stakeholders across the network.

- **Develop new capacity building and training methodologies**

  Thanks to the facilitation of knowledge sharing and community building opportunities, and its holistic approach to capacity building, the R&D Lab could contribute to the consolidation of a growing community of information security trainers, and the development of innovative training resources and methodologies.

- **Contribute to advance organizational data protection protocols and practices**

  By affirming data protection as a critical component of an NGO's security, freedom and power, and by focusing a major part of its efforts on strengthening and streamlining organizational security practices, the R&D Lab could contribute to enhancing the information security of human rights organizations and their extended networks over the long term.

Specific technology research areas

During the course of the interviews, a few specific technology research areas were mentioned by the interlocutors. These were deemed as critical research and development domains to be prioritized in order to most efficiently address the needs of human rights organizations globally.

- **Improving the development and accessibility of encrypted email communications**

  The improved security, accessibility, usability of email encryption would be a critical benefit to the work of human rights organizations all around the world.

  Setting up encrypted email communications channels is still not as straightforward as it should ideally be. When planning the integration of this practice in their operations, human rights organizations report difficulties caused by cumbersome set up instructions,

unclear interface, contradicting information about the alleged security of encrypted email services, and lack of support with the migration from platforms previously used.

Furthermore, encrypted email communications can and should become more secure than they are. One particular aspect requiring further advancement is that currently email encryption is a patch on top of an unencrypted system, encrypting only the message body, and leaving subject line, To, and From fields generally unencrypted, thus making email encryption only partially secure. Mitigating this metadata leakage would be a critical priority of future email encryption efforts.

- **Improving the development and accessibility of secure mobile communications**

  Mobile communications require much-needed improvements in order to become an increasingly secure channel of information exchange.

  Today the challenges posed in this area are numerous. Secure communications alternatives should be available for all kinds of mobile devices. An app on a device cannot be viewed as an all-encompassing solution since the mere presence of a specific app on a device is sufficient for law enforcement agencies in many jurisdictions to prosecute the user. The terms of service of encrypted mobile solutions should not pose threats to the privacy of its user's data.

- **Prototyping secure multi party communications tools**

  Multi-party communications are an essential component of the work of human rights organizations, and the tools currently available do not offer a suitable answer to their security needs.

  What human rights organizations would need are fully encrypted solutions enabling group calls on desktop and mobile devices, complete with audio, video, and chat features. Furthermore, such tools should provide opportunity to connect groups of dozens or even hundreds of users, in order to accommodate different types of calls, from meetings with internal or external collaborators, to video conferences which could, for example, serve as a means to deliver trainings or webinars remotely.

- **Prototyping secure real-time collaboration tools**

  Most of the work done by human rights organizations today happens on digital documents. These files are likely edited and reviewed by more than one staff member, and very likely require authoring and updating in a very short time, or literally in real time.

  The demand for a web-based collaborative real-time editing solution is strong. Such a tool should be fully encrypted for both transmission and storage, offer the opportunity to choose whom to grant access to, and allow to create and work on documents collectively. The ability to create and work on text documents would be essential, along with the need to support spreadsheet documents with those very same features.

- **Prototyping secure first-contact digital solutions**

Individuals and groups whose human rights could be or have been violated need to contact human rights organizations every day, around the clock. Unless they are already in contact with a staff member, and have already set up an encrypted channel of communications to connect securely, a digital first-contact solution to communicate is required.

First-contact digital solutions should be of maximum accessibility and ease of use, encrypted, and built in parallel with a streamlined workflow to process digital rapid response requests.

- **Supporting the development of increasingly secure solutions to browse the internet anonymously, on desktop and mobile**

  As also stated by the 2015 *Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, anonymous technologies are essential to the protection of human rights to privacy and freedom of expression and opinion. Anonymous browsing is an opportunity that thousands of users are already benefiting from. But the room for research and development in this area is tremendous, and its advancement could have critical positive outcomes for the security of human rights organizations globally.

  Ideal future developments of anonymous browsing include richer functionality on both desktop and mobile devices, availability in contexts with very low bandwidth, improved accessibility and usability, and wider adoption worldwide.

- **Divorcing identity and presence from telephony and routing**

  User identity and online presence are currently tightly tied to the infrastructure and information routing that underpins the internet. This makes true online anonymity difficult, and even with good tools like the Tor browser, this decoupling is still challenging and requires constant vigilance.

- **Analysis of the relationship between power and technology**

  Can a user be truly in control of their own communications equipment, and if not, who do they have to cede this control to, and what ability do they have to make those groups act in their best interest? This includes software updates, warrant notifications, software freedom, copyright concerns, naming and who controls names (e.g. what Twitter is doing with the @POTUS handle, as they control that name), and hardware. How do we get to the point where we can tell a story about being in control of our computing machinery?

- **Supporting the development of secure open source operating systems**

  The security measures conventionally taken by the most popular operating systems pre-installed in many desktop and laptop computers, like antivirus programs and firewalls, are unfortunately no longer enough to protect users from sophisticated malware attacks. For this reason, the need for the development of independent, secure and usable open source operating systems is of high-priority.

Secure open source operating systems aim to protect users from surveillance or malicious software, and are designed to be difficult to attack. Being open source contributes to their security as well, since their source code is openly available for others to audit it and suggest fixes and improvments.

Excellent projects are focusing on this need, but the challenges faced in this area of work are numerous. Among them are that resources in support of the efforts in this field are still limited, the research and development required to advance the field would greatly benefit from a wider community of contributors, and stronger connections and cooperation with the corporate sector are essential to be able to prototype and test new solutions.

- **Researching and prototyping secure hardware**

To be able to trust what a program installed on a device actually does, it is necessary to trust the program itself and the operating system running on the device. And to trust the operating system, it is necessary to trust the underlying hardware and firmware it depends on. For decades, hardware and firmware have been generally assumed to be trustworthy, but research on different types of attacks studied in recent years indicates otherwise.

Verifying the security of the hardware manufacturing process is currently as challenging as it is critical. An R&D Lab could greatly support further advancements in this area of research, facilitating the efforts of different stakeholder coordinating their actions. As suggested by one interviewee: "Research and development of secure hardware solutions is at the core of human rights technology. Hardware research and development projects are not easy to fund, because scaling and deployment can be demanding, but it is key for the funding community to understand the critical need of this area for their support. Advocacy organizations could also be of great help, targeting corporate actors manufacturing computer and mobile devices as well as industries that are more under the surface, such as chip and submarine communications cable manufacturers. Furthermore, the entire field would substantially benefit from the work of an entity focused on how to assess and track and report the security of hardware devices, providing open, transparent and accountable information and resources on the subject matter".

- **Supporting the development of increasingly secure whistleblowing platforms**

Whistleblowing, the transfer of sensitive information from inside an organization to a public interest group to expose wrongdoing, is strictly monitored in numerous contexts worldwide, and is targeted with increasingly sophisticated technologies. Whistleblowers, and the members of human rights and press organizations with whom they get in contact, can be put under surveillance, harassed, and in some cases imprisoned.

Secure whistleblowing platforms are a key tool in support of freedom of expression, information and human rights efforts. Today, a few and remarkable projects and whistleblowing platforms are working to advance this area of research, but there is still considerable room for improvement.

A distributed open network of secure whistleblowing repositories could, for example, constitute a potential next step to work towards: the distributed strategy would allow for suitably localized redaction, investigation and reporting of submissions with proper knowledge about their context; the use of open source code would allow for peer review and testing. Furthermore, stronger research and development on forensic analysis, air gap networks, and workflows, usability and adoption of the platforms would be of fundamental help to support the field.

- **Supporting the development and prototyping of holistic organizational security trainings**

  A holistic approach to security can provide tremendous strength to human rights organizations. Addressing physical, psycho-social and digital security of human rights organizations improves the sustainability of their work and their impact.

  The very nature of holistic security trainings creates the opportunity for long term positive change on organizational security culture. It provides organizations with the knowledge needed to assess their needs and vulnerabilities along with the most suitable measures to protect themselves over time. It equips them with a deep and tool-agnostic understanding of their assets, allows them to minimize the effects that ever-evolving adverse scenarios could have on them, and helps them to become increasingly resilient.

  A growing number of digital security trainers across the human rights technology field are researching and applying holistic methodologies to help NGOs learn and put into practice processes guided by this approach. But the practitioners able to provide this service are not nearly large enough in number to address the needs of the human rights NGO sector. An R&D Lab effort could be a well-positioned facilitator to connect different groups and intermediaries working in this field, support knowledge sharing opportunities, and the development and maintenance of of improving methodologies, processes, resources.

Unresolved issues

During our explorations of a potential R&D Lab, interviewees also shared questions and concerns regarding unresolved issues.

Priorities, governance and operations

- **Programmatic priorities**

  The interviewees shared different perspectives with regard to which areas of research and development should be prioritized by the R&D Lab. The following is a summary of the key subjects identified as requiring prompt attention and resources.

  ◦ **Open analysis and documentation of digital forensics**. This was deemed as a research subject still too rarely funded, undertaken and openly shared. Focusing on it would allow to tackle the urgent need to strengthen the sector's ability to identify learnings to build upon and to prototype new and more threat-aware technologies.

  ◦ **User experience and user interface design research for secure tools**. Without timely attention to the integration of UX and UI research as part of technology development, the sector will unlikely be able to achieve a meaningful global adoption rate for secure and privacy-enhancing technologies.

  ◦ **Hardware security**. The production of hardware devices is still largely and dangerously unaccountable, and the ability to use secure software installed on secure hardware is essential to users to protect their data, privacy and rights.

  ◦ **Targeted defense versus mass defense questions**. We can build technologies designed to protect the largest number of people from widespread attack, or we can focus on protecting smaller numbers of people against targeted, sophisticated attacks. It's not clear how to thread the needle; if we do the mass protection, we run the risk of enhancing social inequities. But if we build tools that are designed against higher threat models, we hit adoption barriers due to complexity.

  ◦ **Access to secure technology solutions**. The discovery and adoption of secure technology should become increasingly straightforward, and would allow users worldwide to resist the monopoly of big corporations aggressively distributing alluring but privacy-violating tools.

  ◦ **Integrated technical and legal workflows**. Focusing on this field of research would allow tackling of two issues. It would address the pressing need to develop and distribute technologies with full understanding of the legal scenarios in which they are designed to be used. It would also meet the need of legal scholars and attorneys to achieve the technical understanding needed to oppose legislation and practices which can endanger the privacy and security of human rights organizations and defenders worldwide.

- ◦ **Internet infrastructure**. Failing to dedicate timely resources to researching and advocating for user-centered policies in this field might leave digital rights all around the world at risk to be irreparably violated.

- ◦ **Security training paradigms**. New security trainings designed with a holistic approach and a growing network of trainers able to deliver them would ultimately provide human rights organizations with the most essential support, protection and independence they need when dealing with technology, enabling them to be sustainable and resilient through any technological or societal change.

- **Governance models**

  Interviewees inquired about the governance model that the R&D Lab might adopt. Among the questions raised in this regard:

  - ◦ Would the Lab follow a multi stakeholder governance model, bringing stakeholders together to participate in the brainstorming, decision making, and implementation of solutions to common problems or goals?

  - ◦ Would the project be steered by the decision-making leadership of a designated assembly?

  If the R&D Lab was to become a reality, a survey on different governance frameworks should to be conducted to evaluate which would be the most suitable solution to the project before its inception.

- **Key stakeholders**

  During the interviews, the identity of the R&D Lab stakeholders-to-be was often inquired about.

  Would the project primarily engage with technology developers and designers, technically versed researchers, social scientists, legal scholars, security trainers, human rights organizations, funders or companies? All of them would benefit from the Lab's work, and many of them could maximize their work's impact by receiving coordinated support to collaborate with each other. But would the Lab work with and for all or just some of them?

  Before any step towards its founding, the establishment of a Research & Development Lab would require the identification and prioritization of its stakeholders, and the determination of value propositions and key performance indicators for each stakeholder group.

- **Contributors recruitment and employment**

  A few interlocutors inquired about the type of employment agreements that the Lab would have with the contributors to the projects it would oversee.

  One interviewee shared a reflection in this regard: "It would be very interesting if the R&D Lab could connect with organizations to provide sabbatical leaves for some of their staffers (including financially covering for their absence during that period), thus allowing

professionals to focus on a Lab project full-time for a definite time. This framework could both help projects to get the multidisciplinary skills they require and the entire human rights technology community to build stronger peer to peer support over time".

Sustainability

- **Funding**

  Questions about how the Lab would be funded were raised by all the interviewees.

  As a project with a long-horizon outlook, they noted that it will need to be ensured long-term funding to operate sustainably.

  Interviewees also wondered about the suitability of different types of funds, such as resources solely dedicated to the Lab's work, or shared resources that the Lab could split with other already funded long-term endeavors.

- **Financial and legal identity**

  Interviewees were interested in knowing more about the financial interests of the hypothetical R&D Lab we were talking about.

  More specifically, they inquired about the legal standing of the Lab, asking if it would be established as a non-profit or a for-profit operation.

Intellectual property

- **Open knowledge and access**

  Would the research and development work done at the Lab, as well as the intellectual property generated there, be in any way owned by the Lab itself?

  Such a scenario was deemed in opposition to the fruitful open knowledge exchange seen by all interviewees as one of the most promising results of the Lab's work. A fully open and transparent circulation of the Lab's outcomes would be among the most meaningful and valuable contributions that the project could bring to the sector.

- In any case, whatever the Lab's take on intellectual property, it was common opinion that, with respect to transparency and accountability, the institution should determine and openly state its position before undertaking any project.

Conclusions

Based on the rich discussions that contributed to this report, there is clearly a need and a mandate for some kind of future-focused research and development undertaking addressing the diverse range of technology aspects that impact human rights work and advocacy in our world.

Scoping a time horizon and defining a prioritized remit would be challenging, and the range of possible focus areas borders on overwhelming.

Governance and sustainability also remain unsolved challenges for such a lab, but done right, there is clear potential for real and pervasive impact.

It is our conclusion that the need and the mandate for some type of R&D enterprise are acute and pervasive enough as to warrant further consideration of such a venture.

We welcome conversations in this regard, and are grateful for the opportunity to explore these questions.

Appendix 1: Research Participants

The following is the complete list of interviewees, in alphabetical order.

- Becky Kazansky, University of Amsterdam
- Betsy Beaumont, Benetech
- Bryan Nuñez, Open Society Foundations
- Daniel Kahn Gillmor, American Civil Liberties Union
- Danna Ingleton, Amnesty International
- Fereidoon, ASL19
- Harlo Holmes, Freedom of the Press Foundation
- Isabela Bagueros, Tor Project
- Mahsa Alimardani, Article 19/ Global Voices
- Mallory Knodel, Association for Progressive Communications
- Michael Carbone, Access Now/ Qubes
- Niels ten Oever, Article 19

Appendix 2: Interview Questions

We organized our interview script in two parts.

The first part invited the interviewee's input on general aspects of longer-term thinking; the second part was more specifically focused on the Research and Development Lab concept.

In regard to the latter part of the interview, we specified that the idea was strictly conceptual and intended to drive discussion, and that at the time there were no plans to operationalize any such endeavor.

The following are the questions constituting the first part of the interview:

- Do you think 10 years is a meaningful or useful time horizon along which to consider human rights technology needs? Why or why not?

- Who do you think is already doing good work looking out along farther time horizons for human rights technology?

- What questions do you think need to be addressed in considering the state of play in technology and human rights that far in the future?

- What actions could or should different stakeholders be taking today in order to be better situated in such future contexts?

The following are the questions included in the second part of the interview:

- Does the concept as we describe it make sense to you? Do you have any clarifying questions?

- Do you see value in such a concept? Why or why not?

- To the extent that you see value, what in your opinion would be the most compelling or useful outcomes that such an effort could focus on or produce?

- What concerns or challenges would you identify in trying to model and address future technology scenarios in the human rights context?

- Finally, who else should we be talking to about this topic and these questions?