Toda Peace Institute

JUSTPEACE Labs

Policy Brief No. 125 **March 2022**

Comparing Guidance for Tech Companies in Fragile and Conflict-Affected Situations

Jennifer Easterday, Hana Ivanhoe, Lisa Schirch

Abstract

This research report explores the strengths and weaknesses of four different frameworks tech companies, governments, and civil society can use to assess harms and benefits of new technologies. The four frameworks include human rights, conflict sensitivity, ethics, and human security. The research methodology involved interviews among diverse stakeholders in technology and civil society sectors. This research contributes policy recommendations for developing practical, operationalizable guidance that could have an immediate impact on tech companies' work in countries or regions at risk of human rights abuses and violent conflict.

Introduction

> *[O]nline hate, with the speed and reach of its dissemination, can incite grave offline harm and nearly always aims to silence others. The question is not whether to address such abuse. It is how to do so in a way that respects the rights everyone enjoys.*[1]
>
> - David Kaye

This research set out to explore the following question: What guidance is relevant to how technology companies[2] design, develop and deploy social media and communications platforms in ways that mitigate negative impacts on human rights and conflict? Specifically, this research sought to compare and analyse existing frameworks with a view to finding practical, operationalizable guidance that could have an immediate impact on tech companies' work in countries or regions at risk of human rights abuses and violent conflict.

Tech company activities and their business models impact human rights as well as conflict drivers (which are nuanced and deeply context-specific) both for the better and the worse. As technology becomes more prevalent in our lives and societies, regulation of their unintended negative impacts on human rights and conflict will only become more important, and more difficult. We need an effective framework to build effective governing principles for company policies and procedures on responsible technology and innovation.[3]

The report explores the strengths and weaknesses of four different frameworks tech companies, governments, and civil society can use to assess harms and benefits of new technologies. These include human rights, conflict sensitivity, ethics, and human security. This report evaluates these frameworks as they could or do apply to challenges arising from new forms of technology.

Human rights frameworks focus on individual rights and freedoms endorsed by a wide variety of government, business, and nongovernmental groups. Human rights law offers rules and accountability processes that help companies determine their legal obligations. Many tech companies use human rights law, and the UN Guiding Principles on Business and Human Rights, to make decisions about products and services so that they can avoid violations of human rights.

Conflict sensitivity frameworks include a set of analytical tools for understanding how tech products might negatively or positively interact with fragile or high-risk local contexts. It can serve as a stand-alone framework or "enhance" existing human rights procedures and policies by adding contextual analysis of conflict drivers and impacts. Conflict sensitivity also prompts companies to proactively take steps to contribute to social cohesion and peace.

Tech ethics frameworks help to identify ethical public goods and the development of technology products and services that do the most good for the most people and the least amount of harm. In the public sphere, tech ethics serve as a broad framework for conversation among journalists, academics, and civil society. Within tech companies, ethical "risk sweeping" principles, tools, and processes provide structured methods that anticipate, identify, and remediate social harms and respond to opportunities for increasing social

benefits. It is one of the few frameworks that is broad and malleable enough to address difficult questions about the harms associated with business models.

Human security frameworks describe how to structure public conversation about technology and society, ideally through both public forums and through local multi-stakeholder platforms that emphasise empowerment of local voices and safety of individuals and communities.

Each framework examined in this report had strengths and weaknesses for addressing how technology companies can design, develop and deploy new social media and communications platforms in ways that mitigate negative impacts on human rights and conflict. A common shortcoming was the relative isolation of relevant areas of practice. Although robust in their individual spheres, these diverse approaches are siloed among practitioners. Interviewees for this report demonstrated a nuanced understanding of the benefits and shortcomings of different approaches, but few had familiarity with all of the frameworks or how they would apply specifically at the nexus of social media and technology as they relate to conflict-affected or high-risk situations. Our research shows that there is promise in bringing together the strengths of each framework and building a multi-stakeholder community of practice to address increasingly grave consequences of technology and social media development and business models.

Social Media, Digital Risks, Conflict, and Social Cohesion

Media—whether print, radio, television, or other communications systems—has long been used to cause harm and incite people to violence.[4] For example, the Radio Télévision Libre des Mille Collines spread hate speech before and during the 1994 Rwandan genocide, leading to convictions for the incitement of genocide before the International Criminal Tribunal for Rwanda.[5] However, the emergence of social media platforms and other digital technologies poses new and dire threats to countries around the world. Digital technologies allow false, deceptive, and dangerous speech to spread, target, and influence people at a speed, precision, and scale never before experienced.

Social media's unique characteristics and business model can turn a cell phone or computer into a weapon of mass destruction. Compared with legacy media, digital technology is faster, globally accessible, more affordable, simpler to use, searchable, mostly unmonitored or edited, and offers opportunities for both public and private conversations. Digital technologies enable vast new ways to track a user's location and data. Social media platforms operate largely on a social confidence method of information verification; people endorse information on social media by sharing it with their friends. The rapid growth of new technologies is also unique. New forms of artificial intelligence and machine learning, for example, change social media algorithms that feed unique digital content to each separate user.[6]

A "digital risk" refers to technology that contributes, exacerbates, or creates vulnerabilities. Weaponizable digital technologies cause "digital harms" to individuals, communities, and states, including through:

- Cyberbullying and hate speech that dehumanises individuals or groups (groups using slurs against ethnic or religious minority groups);
- Dangerous speech that threatens individuals or groups with real-world physical violence or harm (gangs or militias calling for violence against an individual or group);
- False or distorted information that leads to health risks;
- False or distorted information that leads to physical attacks on individuals or communities;
- False or distorted information that aims to undermine public trust in institutions or democratic elections; or
- Privacy violations that share personal information in ways that may reveal the location of individuals or communities under threat or enable cognitive and emotional manipulation through cognitive warfare.[7]

These harms are not limited to just areas affected by armed conflict. They are also prominent in other communities that experience a lack of human security or social cohesion, and sometimes act as a precursor to more widespread forms of violence or the emergence of an outright armed conflict. As documented in *Social Media Impacts on Conflict and Democracy: The Techtonic Shift*,[8] Indian social media users spread rumours accusing two men of kidnapping local children, leading to them being killed by a mob. In Brazil, false rumours about a political candidate reached millions of people all over the country on WhatsApp. In Zimbabwe, the government searched social media posts to enforce its ban on critiquing the government. In Northern Ireland, groups of youth sent messages to each other to organise fights along the peace lines that had divided their city. In Colombia, people posted messages spreading false information about the peace process. In Venezuela, the government created an ID system that linked food distribution to social media accounts, suggesting that people who "tweeted" a positive thing about the government might get access to food. In Myanmar and Venezuela, the governments set up troll armies to harness the power of social media in ways that would undermine democracy and human rights.[9]

Perhaps most importantly, many large tech companies operate on a profit model that rewards the amplification of outrage and disinformation. Social media offers users free access in exchange for their attention and data. Tech giants extract private information from users and then sell this information to advertisers, who pay tech companies to target their ads to specific users. Some companies design their products to keep users hooked—or even addicted—to these technology platforms. User attention is at the centre of the profit model. In the "attention economy," tech companies require user attention to extract more private information to sell to political or business advertisers, and to show their ads to more people.[10] False, distorted, hateful, and violent content keeps user's attention. The economic model of many tech platforms correlates profits with user outrage in what some refer to the technology "race to the bottom of the brainstem."[11] The very core of many tech companies' business models can contribute to conflict.

Defining Jurisdictions Impacted by Digital Risks

Digital risks are impacting all countries, but some areas are more at risk than others due to pre-existing factors. This report focuses on the use of digital technologies that amplify the spread of harmful information in "at risk countries" or "fragile and conflict-affected situations" (FCS).[12] This research report does not attempt to define geographic limits related to digital risks. Rather, this report assumes that all four approaches to preventing and addressing digital risks are relevant in most if not all countries of the world where a sizeable majority of the population are using digital technologies. There are a variety of frameworks relevant to prioritising or ranking at risk countries or regions.

At Facebook, for example, staff use a tier system to rank "at risk countries" or ARC. Staff placed three countries—the U.S., Brazil, and India—in the most at risk tier which receives the bulk of Facebook investments of time and resources to form partnerships with fact-checking organisations, devote months of staff time to code machine learning classifiers on local hate speech, and rapid response teams in "war rooms" or "enhanced operations centers" to respond quickly to incitement to violence. The next tier includes five countries: Germany, Indonesia, Iran, Israel, and Italy, and the following tier includes 22 countries. Each tier receives fewer resources than the previous tier.[13] Others may use different criteria for understanding "at risk." For example, in summer 2021, civil society and governments pressed Twitter to restrict the Taliban's use of the platform to coordinate its takeover of Afghanistan in light of the United States' withdrawal of troops. In fall 2021, civil society groups and Facebook staff voiced alarm at how armed groups weaponised the platform to commit genocidal levels of violence in Ethiopia.[14] Thus, some focus on immediate threats of violence and physical harm, and others focus on other types of digital harm stemming from hate speech or misinformation.

At risk countries are by definition complex and dynamic by nature. They involve multiple, interconnected actors, drivers, and motivations; and many are based on long-standing, historical grievances. The absence of overt violence does not necessarily mean there is peace; situations are impacted by invisible social, political, and economic tensions. Situations of social unrest and cycles of violence can emerge with little warning and spark more intense and widespread conflict. Some conflict and human rights issues will be more prevalent in some contexts or developmental phases of a product than others.

According to the United Nations Guiding Principles for Business and Human Rights, described later in this report, companies should undertake "enhanced" due diligence in conflict-affected areas, where the risk of serious human rights abuses is higher. Borrowing from the important contributions of International Alert in this space, below are some examples of how human rights due diligence might differ between stable and conflict-affected or high-risk areas:[15]

- The likelihood and severity of human rights violations is bigger. More rights are usually impacted than many tech companies might be used to evaluating, such as the right to life, right to work, right to health, and right to dignity, amongst others.
- The risks to businesses are greater because of the conflict and the increased difficulty of managing human rights unstable contexts.

- There are more barriers, challenges, and risks involved in stakeholder engagement. Stakeholder engagement will often need to be broader and more nuanced than in stable situations.
- There is a greater chance of unintended consequences, many of which may be difficult to envision or prepare for. For example, despite conducting a human rights impact assessment (HRIA) before starting operations in Myanmar, Telenor did not foresee that its cell towers might be used as bases for snipers, linking the company directly to the conflict and loss of life.

In this way it is vital that a tech company knows when it is operating in a conflict-sensitive setting so that it can appropriately prioritise human rights risks.[16]

However, companies need guidance on defining what a "conflict-affected" area is, and what events should trigger due diligence. Defining conflicts can be tricky and is debated even among conflict experts and scholars. To help, some organisations provide industry-specific guidance and lists. For example, the OECD Due Diligence Guidance includes supplements that provide a list of "red flag" situations related to mineral extraction that trigger the need for enhanced due diligence. Some companies rely on lists of countries that are identified as Fragile and Conflict-Affected Situations (FCS). FCS, as defined by the World Bank, are countries with high levels of institutional and social fragility (such as those with deep institutional crises, poor transparency and government accountability, or weak institutional capacity), and those affected by violent conflict, identified based on a threshold number of conflict-related deaths relative to the population.[17] The UN Working Group on the issue of human rights and transnational corporations and other business enterprises recently laid out four circumstances which should trigger enhanced or heightened HRDD:

1. Armed conflict and other forms of instability, including, among other things, significant political volatility (e.g., sudden regime change), growth in nationalist or other radical movements, the emergence of armed conflict in neighbouring countries, and instability caused by significant poverty and economic inequity.
2. Weakness or absence of state structures, indicated by, e.g., "the lack of an independent and impartial judiciary, the lack of effective civilian control of security forces and high levels of corruption."[18]
3. Record of serious violations of international human rights and humanitarian law, including situations that are recently post-conflict where past conflicts and human rights violations have not been sufficiently addressed through any form of restorative justice or otherwise.[19]
4. Warning signals. This includes, among other things, sustained signs of militia or paramilitary groups, the suspension of, or interference with, vital state institutions; increased politicisation of identity; and, perhaps most notably for our purposes, "increased inflammatory rhetoric or hate speech targeting specific groups or individuals."[20]

Where these triggers are present, the UN Working Group concludes, corporations must adopt heightened or enhanced practices to account for the circumstances and must also

consider certain additional concerns related to engagement with non-state armed groups, the impacts of conflict on women and girls, and responsible exit from a conflict setting.[21]

However, these lists do not always pertain to the technology industry, the unique types of digital harm social media poses, and the lack of human security and social cohesion that may precede "fragility" or violent conflict. There are reports of digital risks in nearly every country on the planet. Even in countries that are mostly peaceful, there are communities and cities within those countries that may face unique digital risks to social cohesion. Using an indicator such as the number of deaths or pre-existing human rights abuses or conflicts may not accurately measure the level of digital risks. While the number of deaths may be relatively low in general, a social media campaign to spread disinformation about electoral integrity could, for example, trigger public protests that could not only be deadly but could put a country's democratic institutions at risk. The costs of digital disinformation and hate speech on public trust in democratic institutions and social cohesion may be putting most or all societies at risk of public violence.

Insufficient Legislation and Legal Regulation

Existing regulation (both formal and informal or voluntary) may fall short in addressing the digital challenges related to fragility, conflict, and social cohesion. Tech companies are generally expected to self-regulate, whether by adopting codes of ethics, human rights due diligence processes, or similar. But these efforts have proven to be ineffective in many regards.

Having clear, enforceable, and rights-based rules would be an ideal approach for mitigating the risks of technology in society, especially as they relate to conflict. However, regulatory efforts to date have largely been reactive, slow, and focused on specific technologies (such as artificial intelligence) or issues (such as freedom of expression). Many jurisdictions are only starting to pass regulations that specifically address the risks posed by social media and other emerging technologies. At the time of writing, there is no international regulation specifically addressing the risks of technology in general or the specific risks of technology related to conflict. Such a multilateral effort remains well outside the realm of political feasibility at the time of writing.

Most applicable legislative and/or regulatory frameworks exist only at the domestic or regional level, although some states and cities are leaders in this space. As such, existing regulations are jurisdictionally narrow – and therefore limited in their ability to address a global problem. There is of course always the possibility that domestic laws which require certain compliance in one jurisdiction or with respect to that jurisdiction's users will lead to wider extraterritorial reach; for example, it was once thought that the implementation of the GDPR might lead to companies applying increased privacy protections for users across jurisdictions. In practice, however, companies are seeking to limit the GPDR rules by moving user agreements to less restrictive jurisdictions.[22]

Mandatory human rights due diligence (mHRDD) legislation, where it exists, refers almost exclusively to conventional supply chains.[23] For example, the UK Modern Slavery Act and the California Transparency in Supply Chains Act apply exclusively to the very specific issue

of forced labour in traditional goods and services supply chains. They do not present much opportunity to address the challenges posed by online platforms in areas affected by conflict. The French Duty of Vigilance Act, on the other hand, is much more broadly applicable across sectors and therefore could present a potential opportunity to advance the respect of human rights by online platforms, although as a practical matter this has yet to be tested.[24] Passed in 2017, it makes French multinational companies civilly liable for human rights violations committed by its subsidiaries, suppliers, and subcontractors, regardless of their jurisdiction. While the first of its kind and an ambitious first step into regulating human rights due diligence, a group of civil society organisations found that in its first two years, the law was ineffective and poorly implemented.[25]

Legal and regulatory efforts that specifically address conflict-affected areas, while well-meaning, can also risk unintentional consequences. For example, the US Dodd-Frank legislation requiring certain companies to disclose their use of conflict-minerals reportedly had negative impacts on the local communities it was intended to protect. [26] Some companies considered that it imposed too significant a compliance burden and weighty risk of legal or financial liability and opted to simply withdraw from those jurisdictions, proving detrimental to those local communities already suffering from conflict.[27] Legislation like this can also open local markets to other, less scrupulous companies – or local militia groups, as reportedly happened in the DRC.[28] While such legislation can have very positive impacts, it also risks exacerbating some conflict dynamics.

With the urgency of quickly developing conflict dynamics, and a world that is increasingly experiencing violence and conflict, another approach is needed to spur action while good, careful, and enforceable legislation is developed. This leads us back to self-regulation, and the need for practical approaches that can help improve business practices while legislators develop legal regulation.

Methods

The research team conducted interviews between May and August 2021 with key experts and stakeholders working within each of these approaches (See Annex 1). We also conducted in-depth desk research. A draft report was shared with interviewed stakeholders for feedback and commentary. Stakeholders also participated in a workshop in September 2021 to address the overall conclusions and key open questions about the research.

Summary of Recommendations

Our research has shown that together, these frameworks provide the necessary components for a comprehensive approach. It is necessary for all relevant stakeholders to come together and work toward the synthesis of a comprehensive approach that considers all relevant frameworks—human rights, conflict sensitivity, tech ethics, and human security—and can inform tech company policies and practices geared toward ensuring that their products and operations do not contribute to or foment violent conflict.

However, much progress is required to get there. There is an urgent need for action and work on this issue. We have highlighted the following recommendations for industry, civil society, academia, and donors:

1. Define what types of indicators related to conflict would trigger enhanced responsibilities.
2. Understand what "enhanced due diligence" is and would require.
3. Distinguish between types of impact on conflict.
4. Create a community of practice and expertise that does not just include but elevates stakeholders from local communities.
5. Support community-based and co-created processes for anticipating and analysing tech impacts and harms and developing appropriate remedy.
6. Curate a set of case studies that identifies both failures to anticipate harm as well as cases that illustrate good practices.
7. Offer incentives and a reward structure for technology staff and companies that illustrate best practices in ethics, human rights, conflict sensitivity and human security.
8. Look to lessons learned from other sectors for best practices for implementation.

Human Rights

Grounded in the Universal Declaration on Human Rights and other international human rights treaties,[29] the United Nations Guiding Principles for Business and Human Rights (the UNGPs) codified the "protect, respect, and remedy" framework that has guided companies in the improvement of their human rights policies and practices over the last decade.[30] The UNGPs have become "the global standard of practice that is now expected of all states and businesses with regard to business and human rights,"[31] pursuant to which companies must "address adverse human rights impacts with which they are involved."[32]

Until relatively recently, the UNGPs were viewed largely as a voluntary normative framework that socially responsible companies might opt to follow, but for which there was no real mechanism for enforcement or accountability for failing to comply. Companies were motivated to follow (or to attempt to appear to follow) the UNGPs by the reputational risk of being linked to a human rights violation. However, with the emergence of mandatory human rights due diligence legislation across some jurisdictions, some companies have begun to view minimum human rights compliance as a legal requirement.[33]

One helpful way to think of a business and human rights framework is that the UNGPs provide the structure and procedures by which industry is to be held to the human rights standards embodied in the Universal Declaration and the various subsequent human rights instruments that further codify those standards.[34]

Relevant Human Rights Instruments and Initiatives

Universal Declaration on Human Rights

In 2018, the UN Human Rights Council (HRC) unanimously passed a resolution on "the promotion, protection and enjoyment of human rights on the Internet" which affirmed that "the same human rights that people have offline must be protected online."[35] Although a survey of all applicable human rights instruments is unfortunately outside of the scope of this analysis, a brief discussion of some of the more salient provisions of the Universal Declaration can shed light on the underlying standards constraining company behaviour pursuant to an application of the UNGPs. Article 29 is particularly salient to the problem of emerging technologies as they relate to conflict.

Article 29 of the Universal Declaration establishes that rights protected under the Declaration are not absolute and may be abridged in a narrowly tailored and limited way where and when necessary, to protect the rights of others.[36] This "proportionality" rule allows the infringement of fundamental rights in some circumstances. Many states and companies have used fighting terrorism or child exploitation to abridge basic human rights, including the right to privacy and freedom of expression. Article 29 is also notable for its acknowledgement of the duty we all have to other people, by which, according to UN commentaries on the Guiding Principles, each of us "should protect their rights and freedoms,"[37] and that the "rights of each are therefore limited by the rights of others."[38] Article 29 has become particularly important with respect to government regulation on content moderation.

Article 19 protects the freedom of expression. But as discussed above, this right must be balanced against the duties and limitations codified in Article 29. The interplay between Articles 19 and 29 raises significant issues of concern with respect to social media contributing to harm and violence offline. Leading business and human rights consultancy, Business for Social Responsibility, observed this inherent tension in its recent primer on human rights priorities for the ICT sector:[39]

> [G]overnments are increasingly interested in proactive monitoring, surveilling, removing, and blocking of certain types of content, especially terrorist content and dangerous speech. These content restrictions are important for human rights protection but must be "necessary and proportionate" and the least intrusive restrictions to achieve the desired result. Access to appeal and remedy in the event of over-blocking is crucial.[40]

In this way, the Universal Declaration tells us that companies must do what they can to ensure that the design, deployment and ultimately end-use of their technology respect citizens' right to freedom of expression, while at the same time balancing that right against the rights of others who might be threatened or otherwise adversely impacted because of that expression. While this undoubtedly provides additional parameters to assist in triangulating the exact scope of company duties vis-a-vis the content on their platforms, it still fails to provide the affirmative, proactive guidance on what exactly that looks like for platform companies as they go about the process of product design and deployment.

U.N. Guiding Principles (UNGPs)

Under the UNGPs, "respect" for human rights requires companies to avoid directly causing or contributing to adverse human rights impacts, as well as to "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."[41] This "cause, contribute, directly linked" attribution schema is one of the biggest strengths, and also shortcomings, of the UNGPs. While it provides a clear structure for companies to understand their human rights impacts, it also constrains thinking about the relationship between corporate activities and societal impacts that may not be easily captured by specific substantive human rights laws.

Indeed, even just linking technology companies' products and services with human rights abuses is challenging and under debate. Some clarity on this is starting to emerge, as the tech industry is increasingly implicated in serious human rights abuses and violent conflicts. For example, with respect to the role of Facebook in the Myanmar conflict of 2016 and 2017, John Ruggie said:

> When can we say that a company like Facebook is 'contributing to' human rights harm?... Unwittingly getting even severely consequential cases wrong once or twice is one thing. But persistent refusal to substantially change what the company does to reduce its role in others' promotion of social strife and violence makes the attribution of 'contribution' inescapable.[42]

Principles 17 through 20 of the UNGPs outline in explicit detail the type of human rights due diligence that is needed to ensure that companies are abiding by their duty to respect. Specifically, companies must not only produce and comply with meaningful policies for the respect of human rights, but must also engage in affirmative human rights due diligence practices that include:

1. assessing actual and potential human rights impacts (through human rights impacts);
2. integrating and acting upon the findings, tracking responses; and
3. communicating how impacts are addressed."[43]

UN Human Rights' Business and Human Rights in Technology Project

Noting the unique challenges of applying a business and human rights framework to the ICT sector, UN Human Rights' Business and Human Rights in Technology Project (B-Tech) is in the process of a multi-step, multi-stakeholder project to determine what it means to specifically apply the UNGPs to digital technologies with respect to both i) addressing human rights risks in business models and ii) human rights due diligence and consumer end use.[44]

In connection with the launch of the B-Tech project in 2019, David Kaye, the former UN special rapporteur for freedom of expression, identified three discrete areas that companies

should focus on to address the amplification of dangerous speech leading to potential violence and human rights abuses:[45]

1. HRIAs at all stages of product design and development;
2. The vagueness of company rules; and
3. The lack of transparency around company processes.[46]

A B-Tech paper, Addressing Business Model Related Human Rights Risks, confirms that the UNGPs are to apply to "situations in which business model-driven practices and technology design decisions create or exacerbate human rights risks." These situations are common for many tech companies, including the social media platforms exploited for divisive and sometimes violent ends.[47] The paper further found that:

> The increasing reports of technology's role in exacerbating human rights harms have thrown into sharp relief the prospect that individual incidents are not so much outliers as somehow built into the logic of how the business of technology has been constructed and evolved.[48]

More specific to the precise issue of the weaponisation of social media, online platforms have organised their business models around the use of "algorithmic systems that manufacture virality and preferentially—if unintentionally—promote content that contributes to online and offline human rights harms and grave human rights abuses."[49]

To ensure adherence to the UNGPs in these situations, the B-Tech paper advises:

1. Revisiting performance incentives for top management and design personnel to reward the prevention and mitigation of human rights harms and not just the maximisation of revenue;
2. Scrutiny of new business markets (before they are entered) to pre-emptively determine whether local contexts might lead the tech being introduced to exacerbate conflict or human rights abuses;
3. Engagement in meaningful collective action initiatives that encourage a consultative process for ensuring respect of human rights; and
4. Advocacy for legislation and regulation that helps protect the human rights the company's business model may put at risk.[50]

Ultimately, the B-Tech project has made it clear that there is no tech exceptionalism when it comes to human rights:

> The Guiding Principles apply equally to all businesses in all sectors. For example, there is no fundamental difference in outcome between a mining operation faced by the challenge of known local militias using their trucks to attack, rape and kill members of a specific community and a social platform allowing known extremists to post hate messages inciting the attack, rape and killing of members of a specific community. Second, the sector should adopt a genuine human rights approach, in which all rights are recognized as equal, rather than a misguided understanding of human rights whereby

> the right to free speech, or the right to physical security, would be so absolute or unyielding as to trump any other human rights.[51]

It is encouraging to see the UN take up the issue of how precisely to apply the UNGPs to the unique characteristics and requirements of the tech industry. But the B-Tech project has been unable to fully and comprehensively address how to operationalise and implement the human rights risk mitigation promise of the UNGPs to such a complex and rapidly changing industry. Take for example the recommendations above: if a business model dictates that a platform utilise algorithms to maximise the number of times content from a user is shared, thereby increasing user engagement and subsequently advertising revenue, how could that same company build financial incentives into its employee review process that discourage the very type of practice on which its business is based?

Other Guidance on Implementation of Human Rights Principles

In July 2020, the UN Working Group on the issue of human rights and transnational corporations and other business enterprises issued a report entitled "Business, human rights and conflict-affected regions: towards heightened action." The report lays out practical measures that companies should take to "prevent and address business-related human rights abuse in conflict and post-conflict contexts, focusing on heightened human rights due diligence and access to remedy."[52]

The new report seeks to fill a significant need for further guidance on how to implement the UNGPs in a meaningful way for companies affecting fragility and conflict in countries around the world.[53] The UN Working Group recognised that more was needed "to help ensure that business does not stimulate or exacerbate conflict or negatively impact peacebuilding."[54] The report notes that although the UNGPs do not explicitly require heightened or enhanced HRDD as they relate to conflict, nor specifically mention a different type of due diligence in those contexts, they are based on the concept of proportionality, where higher risks require more robust HRDD should be. Logically, then, because conflict-affected areas pose heightened risks of human rights abuses, companies should similarly undertake appropriately "heightened" due diligence.[55] The severity analysis, which is provided for in the text of the UNGPs, operationalises this principle and provides some insight into how to respond to situations of heightened concern or intensity in which two rights are in conflict or competition.[56] As a starting point, companies should implement thorough, regular, and iterative processes of stakeholder engagement and HRDD (including risk assessments) to ensure that they are aware of often rapidly changing circumstances related to fragility, conflict, social cohesion, and the potential for violence.[57]

The report also addresses the unique challenges the tech industry faces when doing business in countries experience conflict or fragility. The UN Working Group acknowledges that significantly more research is needed to understand the full scope of human rights implications for tech companies entering those markets, but also provides some concrete guidance for certain tech sub-sectors, ranging from autonomous weapons of war to mis- and dis-information campaigns on online platforms.

The report suggests that ultimately a multistakeholder initiative geared toward better understanding the implications of the UNGPs applied to the tech industry in this context is a vital next step:

> If there is no doubt in relation to the normative framework, much work remains to be done to flesh out the concrete consequences of implementing the Guiding Principles for this industry. A multi-stakeholder initiative bringing together representatives of industry, States, and civil society, with the overarching objectives of operationalizing the human rights responsibilities of the sector, and setting out practical guidance and standards for the responsible provision of cyberservices, would seem to be particularly timely.[58]

The report is helpful for understanding human rights obligations for tech companies doing business in FCS. First, it clarifies that the UNGPs and all of their responsibilities apply as much to tech as to other industries: "there is no exceptionalism for the sector."[59] And second, the report calls for equal protection of all human rights, stating that the tech industry must "adopt a genuine human rights approach, in which all rights are recognized as equal, rather than a misguided understanding of human rights whereby the right to free speech, or the right to physical security, would be so absolute or unyielding as to trump any other human rights." [60] Notably, however, the report fails to define exactly what is envisioned by heightened or enhanced due diligence and therefore fails to adequately instruct companies on how to ensure that they are conducting the necessary due diligence to be assured they are respecting human rights in the countries in which they operate. More is required in terms of augmentation of the UNGPs in a manner that is practically implementable.

The Rabat Plan of Action

First adopted at an Office of the High Commissioner of Human Rights (OHCHR) expert workshop in 2012, the Rabat Plan of Action offers perhaps the most detailed and directly on-point guidance on the implementation of a framework for the balancing of freedom of expression on the one hand versus hate-based violence on the other.

The Rabat Plan of Action created a highly practical and operationalizable six-part test for determining hate speech likely to incite violence and therefore subject to limited restrictions to freedom of expression: "(1) the social and political context, (2) status of the speaker, (3) intent to incite the audience against a target group, (4) content and form of the speech, (5) extent of its dissemination and (6) likelihood of harm, including imminence."[61]

Although still one of the lesser known human rights instruments of relevance here, the Facebook Oversight Board invoked the Rabat Plan of Action in completing its recent analysis of the suspension of Donald Trump's Facebook account in the wake of the January 6 riots on Capitol Hill.[62] In fact, the Board evaluated the decision to suspend Trump's account and the speech in question leading up to that suspension through an examination and application of each of the six factors the Rabat Plan outlines. Finally, the board stated that it relied on the Rabat test in reaching its conclusion that the violation in that case was severe

in terms of human rights harms, and the account restrictions imposed by Facebook necessary and proportionate.[63]

Experts in this area, however, caution that the Rabat Plan is not without its flaws. Particularly, some have cautioned that "imminence" and "intent" criteria are problematic for analysing when it might be appropriate to remove content for the prevention of violent conflict. According to Susan Benesch of the Dangerous Speech Project, the imminence requirement is particularly concerning. She argues that "if companies wait to respond to dangerous content until mass violence is imminent, it is usually too late to prevent it."[64] With respect to the intent requirement, it is also debated whether it should be necessary for a poster of content to intend to conflagrate violent conflict or whether instead it should be sufficient for a platform to pull any content that has that effect. Benesch also raised concerns around the difficulty of discerning intent and its variable nature: "frequently the person who originates inflammatory content intends to incite violence, but people who share it do not–or vice versa."[65]

Strengths

The UN has already done the heavy lifting to enable a human rights approach. Extensive research and stakeholder consultation have gone into the drafting and endorsement of first the UNGPs themselves, and the subsequent B-Tech project and UN Working Group reports on the issue of human rights and transnational corporations and other business enterprises in conflict settings.[66] We now have the frameworks outlining not only the corporate responsibility to respect human rights—across all sectors and in fragile and conflict-affected settings—but increasingly a blueprint for what the respect of human rights requires when tech companies enter those high risk settings. As compared to competing frameworks for responsible tech, a human rights approach is significantly more advanced in its development.

Industry is already on board with a human rights approach. Despite some outlier resistance, "human rights" has effectively become the official language of corporate social responsibility. It has increasingly been applied to the unique circumstances and business practices of the tech industry in a way that seems to have proven compelling for industry leaders.[67] Industry is already familiar and comfortable with this approach and its procedures. This sentiment was echoed repeatedly by stakeholders interviewed as part of this analysis; many of those same stakeholders expressed concern that asking the companies to stop course in an area they have been encouraged for years to pursue and start something entirely new could deter industry commitment.

The UNGPs and the Rabat Plan of Action already provide practical tools to navigate situations in which rights conflict. In fact, a human rights framework is arguably the only framework suited to advise on how to proceed where the respect of two different fundamental rights are necessarily at odds. Although the UNGPs do not explicitly address what to do in instances of competing rights, e.g., freedom of expression vs. right to life, they do provide for the use of a "severity analysis" in order to reasonably determine which right should take priority where there are two competing or conflicting rights at issue.[68] The Rabat Plan of Action also provides for an easily operationalizable six-part threshold test to

determine when online speech reaches the level of hate-based incitement such that it should be subject to certain freedom of expression limitations.

Human rights can work alongside other frameworks to address the amplified risks and threats when operating in FCS. The UN Working Group report discussed above provides a roadmap for how a business and human rights framework and a conflict sensitivity approach can be integrated. There is also increasing awareness about the need for tech companies to adopt enhanced due diligence and conflict awareness. Noting that, despite good faith efforts, "businesses are not neutral actors; their presence is not without impact,"[69] the B-Tech project acknowledges the complexity in addressing rights-respecting business activities that nevertheless exacerbate conflict.[70]

Human rights have more options for enforcement. While often critiqued for its lack of teeth, a human rights framework poses significant advantages when compared to an often infeasible legislative or regulatory framework. Human rights is both inherently more international in nature (in the absence of a multilateral treaty) with almost universal acceptance,[71] and also poses significantly less risk of principle proliferation while still providing a meaningful framework for platform governance.[72] The application of a human rights framework in place of a traditional legal approach can also deter forum shopping, which is a risk of piecemeal legislation.[73] To date, efforts to regulate the fast-moving tech industry have been all too "isolated, reactionary, and flawed."[74]

At the same time, a human rights framework shares some of the attributes of a traditional legal or regulatory framework. It is binding, based on rule of law, and is verifiable, specific, and detailed. It is an international system, based on a commonly understood language, and includes a broad range of procedures and institutions to help protect rights and provide adequate remedy.[75]

Weaknesses

Local stakeholders and beneficiary communities are frequently left out of the HRDD practices that companies use to implement the UNGPs. This vulnerability speaks perhaps less to a weakness of the UNGPs as a framework, and more to a problem with how they have been implemented to date. There are also, in fact, increasingly alternative approaches to HRDD that consider or are organised around beneficiary community experiences and input.[76]

HRIAs generally must be comprehensive, robust, and regularly revisited overtime – but in practice, usually are not. They must be extremely thorough and complex and address multiple features of each technology product or service, particularly in FCS. For example, some criticised the Facebook Myanmar HRIA because it failed to assess the role of Facebook's News Feed algorithm.[77] HRIAs should also be conducted in an interdisciplinary manner, involving social scientists, computer scientists, and engineers.[78] This is especially true for HRIAs in FCS – it takes a wide range of experts and knowledges, including those of impacted communities, to understand the impact of technology on conflict and what would be an appropriate action to mitigate risks of harm and take proactive steps towards building peace and human security.

Also, as currently executed, many HRIAs fail to engage with long-standing and historical conflict drivers or tensions. For example, Facebook's HRIA in Myanmar failed to connect key elements of the conflict—such as the longstanding discrimination against and oppression of the Rohingya—with decisions on how Facebook's feed was deployed and operated. As Data & Society notes, the Facebook-commissioned HRIA does not evaluate how this

> specific ethnic tension and history of oppression set the baseline conditions upon which its platform would be used. … The UN Guiding Principles propose that companies should prioritize addressing the most severe human rights impacts. The treatment of the Rohingya should be the first place that any HRIA in Myanmar begins.[79]

Meaningful efforts at tech company HRDD are often stymied by company opaqueness and an industry-wide lack of transparency. Black-box algorithms and artificial intelligence (AI) systems can make it difficult to assess impacts on human rights as well as assigning responsibility and accountability. This pertains to understanding the inner workings of relevant algorithms – corporate policies require engineers to "show their work" through documentation, so that things like an AI system's reasoning behind its decision-making are readily apparent.[80]

Conflict Sensitivity

Conflict sensitivity tools are another approach relevant to addressing digital risks in FCS. Any organisation, company, or programme operating in a conflict-affected context is very likely to have unintended impacts on that situation. Conflict sensitivity frameworks draw upon conflict analysis or conflict assessment processes from the field of peacebuilding to improve the ability to predict and avoid potential harms while maximising social goods.[81]

To be "conflict-sensitive," a company should be able to:

1. Understand the context in which it operates;
2. Understand the interaction between its activities and that context;
3. Take steps to minimise the negative impacts of its operations; and
4. Take steps to maximise the positive effects of its operations for peace.

Conflict sensitivity tools were developed for UN and international NGO programmes in humanitarian assistance, development, and peacebuilding.[82] These types of organisations use conflict sensitivity frameworks to analyse what are commonly called "dividers" and "connectors": elements in society that divide people and are sources of tension, and elements that connect people and are local capacities for peace.[83]

Over the last two decades, conflict sensitivity tools have been adapted for companies doing business in FCS, such as extractive or security companies, or companies whose supply chains include conflict minerals. Conflict sensitivity has increasingly been applied to business and is now a central aspect of the UN Global Compact, a UN initiative for business commitments to sustainability principles. Conflict sensitivity frameworks offer businesses tools to operate responsibly and to mitigate the risk that their operations might contribute to conflict.[84]

There are several resources available for companies that want to apply the conflict sensitivity framework. For example, the United Nations Global Compact offers a relevant and highly practical Business Guide to Conflict Impact Assessment and Risk Management that seeks to ensure conflict-sensitivity at both the preoperational and operational stages of investment.[85] The Guide contains certain key questions for businesses to answer before they enter and as they continue to operate in conflict-sensitive markets. Each question touches on a particular risk factor that can or is likely to contribute to conflict.[86]

However, almost none of these tools are adequately tailored to the technology industry and its unique business models. Effectively all the literature, frameworks and company guides for integrating conflict sensitivity into business operations seem to refer exclusively to traditional business models, with a heavy focus on the extractives and private security industries. There are significant gaps with respect to issues faced by the tech industry in general and social media and communications platform companies specifically.

JustPeace Labs has sought to fill those gaps with its work on conflict sensitivity for the tech industry. Recognising the unique challenges faced by technology companies—such as the scale, scope, global reach, and rapid pace of development—we have developed a research programme and suite of tools to help the industry adopt conflict sensitive practices and enhance existing human rights and ethics programmes.

For example, JustPeace Labs's advice on conflict sensitivity includes the following:

1. Conduct a detailed conflict analysis and identifying how the company's technology products and services impact the conflict. This should also include analysis of algorithms, business models, and understanding the nexus between the conflict impacts and the relevant technology, partners, clients, and users;
2. Identify ways that the company can prevent and mitigate adverse impacts on conflict and making sure that other human rights mitigation steps won't have a negative side effect on the conflict. This may be different from impacts on human rights, and sometimes efforts to mitigate negative human rights impacts can in turn negatively impact the conflict;
3. Bring a conflict sensitivity lens and experience into human rights grievance mechanisms, and community engagement strategies and programs; and
4. Protect the safety and security of rights-holders during high-risk due diligence processes.[87]

Conflict sensitivity takes a broad approach to identifying impacts and harms by not just looking at harms related to specific rights, but also considering those most impacted by or vulnerable to conflict and others that are affected by the conflict.[88] It is focused on outcomes, rather than specific rights, and thus is unconstrained by issues of attribution or apportioning responsibility. It is primarily centred on how business activities impact conflict, social cohesion, and strengthening peace. As a result, conflict sensitivity analyses tend to be highly relational and contextualised, based on understanding the relationships between different actors in society and the company.[89]

Conflict analyses focus on mapping and understanding complex dynamics of a conflict. They are best conducted with significant on-the-ground stakeholder engagement and should be frequently revisited. They involve looking at key actors in the conflict, including who are key peacebuilders (connectors) and who might be spoilers (dividers). Looking at the history and motivations of different stakeholders is also important, including among diasporas. Understanding conflict dynamics also includes a deep dive into political, economic, and socio-cultural contexts, including as they differ across geographies. This frequently involves a history of serious grievances or perceived grievances, such as colonialism, discrimination, power asymmetries, mass human rights abuses, and/or slavery. It also frequently involves a long political history of involvement by foreign states and organisations.

For example, researchers might conduct focus groups, interviews, or mobile surveys on the following types of questions:

- Who are the main groups in society and where are their lines of division or alliance? Who will have influence in how digital technologies will operate in a certain country? Do they enjoy popular support? Who are political opponents of the current government? Who are the main civil society leaders? Who are the primary users of our technology in this area? Who are the relevant vulnerable groups impacted by our technology and/or the conflict? Who are the primary online influencers in this context?
- What are the most salient conflict drivers? How do they relate to or are impacted by technology? What are the possible unintended impacts of a technology on a society? What are the relevant human rights impacts associated with those conflict drivers? What have been precursors to flareups of violence and a reduction in social cohesion? How is that influenced by technology?
- How is technology influencing this conflict? Might leaders be able to use digital technologies for surveillance of political opponents or attempt to use their power over technology to spread disinformation to hold onto power? How might technology companies design their products and policies to make such negative uses less likely?
- When are the most likely times of the year that public violence might break out, based on the calendar of holidays, anniversaries, elections, or political transitions? When is enhanced due diligence necessary?

Conflict sensitivity due diligence helps companies identify the risk that a company will either create new or exacerbate existing conflict drivers through their business activities. It can also raise human rights impacts that map onto those conflict risks.[90] A conflict sensitivity analysis can highlight additional risks and human rights impacts that might not be captured by a typical HRIA.[91] For example, while a human rights analysis might note that a content moderation decision is necessary to protect the right to free speech, a conflict sensitivity analysis looks at how the permitted speech may impact the conflict, even if it does not violate content moderation policies. If there is a risk that it exacerbates conflict, that may be a reason to restrict speech in certain circumstances. What is more, conflict sensitivity focuses not just on mitigating risks but also how companies can make positive contributions to peace and stability.

Conflict sensitivity may require more frequent analysis, as conflict situations are subject to change rapidly and unexpectedly, depending on the volatility or dynamics of the conflict. It may also require drawing on different types of experts than is typical for a human rights assessment, such as anthropologists, sociologists, or historians.

Strengths

Conflict sensitivity is based on understanding relationships between stakeholders and takes a systemic view of complex situations. Conflict sensitivity is the only framework in this study that deals with the complexity and nuance of FCS and asks companies to understand their role as conflict actors. This analysis can add to a deeper understanding of other issues as well, such as human rights, environmental impact, employee relations, and human security.

Conflict sensitivity fills gaps regarding conflict analysis in other frameworks. Conflict sensitivity provides a framework for doing additional analysis that can inform other frameworks with significant blind spots regarding conflict and FCS. In FCS, state structures are often weak or non-existent, and therefore human rights protections usually do not work as intended.[92] Companies cannot expect that they will be operating within a regulatory system that protects human rights. Indeed, human rights violations may be part of the social fabric of FCS.[93] The UNGPs stress that there is a heightened risk that companies will become involved in particularly severe human rights violations due to a lack of awareness of complex contextual dynamics such as political, social, and economic features of the situation.[94] Once a company becomes linked to human rights violations or violence in an FCS, human rights risks can escalate quickly. These human rights impacts may be difficult to foresee during previously conducted HRIAs if those HRIAs failed to incorporate conflict sensitivity principles. Conflict sensitivity analysis informs HRIAs, understandings of the human rights context, impacts, and mitigation and remedy strategies.[95] Conflict sensitivity can also build in more responsiveness to conflict triggers and areas where more frequent assessments would be necessary.[96]

Conflict sensitivity is easily integrated into other analyses and frameworks. Conflict sensitivity can be simply integrated into other framework analyses and in fact, serves to strengthen them by deepening understanding, surfacing challenges, and connecting closely with stakeholders and communities. Indeed, integrating conflict sensitivity into existing protocols is both more practical and can have more value than engaging in two separate processes.[97] This would reduce inefficiencies and allow for contextual and nuanced thinking in assessing a spectrum of approaches a company can take in these situations. It helps companies identify measures they can take to avoid becoming involved in conflict, and opportunities to contribute to social cohesion and peace. Conflict sensitivity can also help ensure that the human rights due diligence process, and the actions recommended, are themselves conflict sensitive.

Conflict sensitivity can highlight trade-offs that might need to be made in evaluating human rights impacts and other compliance challenges. In some FCS, certain rights might need to be compromised temporarily to avoid exacerbating conflict. For example, as Graff and Iff note, “integrating marginalized communities into consultative processes and joint decision-

making may fuel conflicts between different society groups."[98] An integrated approach will make these dilemmas come to light and help companies develop sound policies and procedures for navigating these complexities.

Conflict sensitivity calls for proactive action to support peace. While other frameworks focus on mitigating risks or the idea of "do no harm," conflict sensitivity emphasises taking positive steps towards peace. In asking companies to understand and analyse their roles as conflict actors, this also allows for thinking and action about how to use that role to reduce conflict overall. It has a broader impact on the whole of society, not merely on groups whose rights might be directly impacted by company activities.

Weaknesses

Conflict sensitivity as a framework overall does not include an accountability mechanism, either for remedying harms or for holding a company accountable for its conflict sensitivity processes or lack thereof. It is difficult to quantify or measure the results of a conflict sensitivity process or whether a company was successful in mitigating negative impacts on a conflict or not.

There is a general lack of awareness about conflict sensitivity outside peacebuilding practice. Many stakeholders were unaware of the intricacies of a conflict sensitivity analysis. While awareness that FCS need to be considered distinct from other markets and contexts, human rights and ethics are still the dominant ways of thinking about the risks of technology in society. As such, conflict sensitivity can be considered an additional burden, and as unnecessary if a company already has a human rights due diligence programme.

Conflict sensitivity may also create additional friction or contribute to inaction. Technology companies are not accustomed to thinking of themselves as conflict actors. They do not typically have offices located directly in FCS, or have business activities that involve security forces, armed groups, or conflict-affected communities. Despite the growing recognition among social media and platform companies that their activities can impact conflicts, the idea that technology is neutral is still pervasive. Asking companies to undertake conflict sensitivity analyses, or to publicly acknowledge conflict sensitivity processes, can give the impression that they are already perceived negatively, rather than as potential peace builders. It may also raise alarm that they could be opening themselves up to potential responsibility in some form for past conflicts that have occurred. Furthermore, companies could perceive proactively taking on peacebuilding activities and supporting peace as complex and risky, and easy to get wrong. As such, many companies may simply choose to "park" conflict sensitivity as a framework that does not receive the attention and implementation that is required.

Tech Ethics

While there are numerous competing definitions of ethics and different ethical approaches, for the purposes of this paper ethics broadly refers to standards of human behaviour that both maximise benefits and attempt to prevent, minimise, or eliminate harms.[99] But the

concept of ethics means different things to different people. One interviewee critiqued ethics as an "inkblot … it is whatever you think it is." In some settings, people view ethics as an overly broad philosophical approach, or one that lacks practical application in a business setting.

Everyone agrees on one point: ethics are distinct from laws and regulations. Some interviewees defined ethics as the public dialogue that takes place outside of formal rules and regulations where the public can identify potential or actual harms from technology. Ethics requires public discussion because there is a lack of clarity in existing frameworks, and new technologies are rapidly creating new, unanticipated consequences. In her podcast interview on tech ethics, Elizabeth Renieris notes, "we just have to be careful that we don't wait for regulation. One of the things that I particularly like about the technology ethics space is that it takes away the excuse to not think about these things before we're forced to."[100]

While regulations include a set of "how" questions related to "how will governments regulate tech companies" and "how will companies be held accountable?" ethics pose "what" questions including "what are the positive and negative impacts of a technology on individuals and the wider society?"

Another interviewee pointed out that ethics also addresses questions of implementation, as existing regulations, laws, or human rights frameworks do not always adequately explain or cover new technologies or the nuances of how an existing regulation and human rights framework might apply to a new technology. Existing regulations do not provide adequate guidance for the scale and scope of harms experienced in conflict-affected situations.

Others view ethics as a set of professional behavioral expectations. Tech companies have been creating ethics portfolios, hiring people to be ethics "owners" who will hold responsibility for integrating ethics frameworks throughout the organisation and throughout the project life cycle.[101] Toolkits and processes have proliferated under various banners, asking teams to undertake processes for "responsible" innovation. Yet ambiguity and a lack of a unified understanding of ethics continues to linger.

Ethics principles and processes ask broad questions about the design, profit model, governance, and regulation of technology. Currently, tech companies have few legal restraints related to their design, functionality, and algorithms of their platforms. Therefore, ethics can serve to fill some of those gaps.

Relevant Tech Ethics Principles, Tools, and Processes

There are a variety of different efforts to establish ethical principles for technology. Several leading technology companies and universities have set up initiatives to explore the ethics of AI technologies. Tech companies recognise that failing to anticipate negative impacts of AI exposes them to "reputation, regulatory, and legal risks" as well as "wasted resources, inefficiencies in product development and deployment, and even an inability to use data ."[102] The challenge is that academics can list abstract values, but lack the ability to translate them into practical guidance for tech engineers, designers and teams and may fail to take into

consideration corporate profit goals that drive tech innovation. If tech company engineers and teams develop ethical principles, their monoculture is so removed from real-world concerns that they fail to anticipate worse case scenarios or even obvious practical implications of new technologies.

The Markkula Center for Applied Ethics at Santa Clara University directs a programme on "Ethics in Technology Practice" that publishes a variety of ethics toolkits and publications on best ethics practices for tech companies. Drawing both on academic and tech experts, the Markkula Center encourages viewing technology as a form of power. To be ethical, technology must serve the interests of life and the public good. At every stage of tech product work cycles, tech ethics ask "Will this produce the most good and the least harm?" "Does this respect the rights of all of the relevant stakeholders?" "Does this treat people fairly?" "Does this serve the community as a whole, not just some of its members?"

The Markkula Center advocates that tech ethics requires daily, ongoing, pervasive, iterative questions built into the structure of every conversation and meeting about technology in every phase of design, implementation roll out, and evaluation of a tech product. Tech ethics is not a one-time "box to check" focused on minimal "compliance mindset" that views ethics as an external requirement. Instead, tech companies should view ethics as an "integral part of being good at what we do."[103]

The Markkula Center's list of tech ethics areas of concern includes broad questions of data privacy, the transparency of algorithms, and tech designs built on the "attention economy." The Markkula Center also explores specific concerns related to FCS, including digital psychological manipulation, surveillance, and declining social trust.[104] Markkula Center's list of best ethics practices includes the following relevant advice for FCS:[105]

- Be mindful of the impact of technology on human lives and interests, including how technology affects people's bodies, finances, relationships and emotional or mental states.
- Anticipate a range of worse case scenarios of how people might use technology in ways that cause harm and risks.
- Be wary of false assumptions that there are technological solutions to ethical challenges related to technology. Technology is not "a silver bullet for complex social problems."[106]
- Identify a person or unit responsible and accountable for each aspect of ethical risk management.
- Practice disaster planning and crisis response to anticipate how they might respond to a variety of worst-case scenarios.
- Invite diverse stakeholders to offer input to identify potential risks of technology products and how technology can be designed to contribute the most toward human well-being. Diverse stakeholders are essential to avoiding the psychological problems of groupthink and blind spots that occur when tech companies rely on people of similar gender, race, ethnicity, age, education, and geography to design products that will be deployed around the world in contexts these tech designers cannot understand or anticipate given their identity and circumstance.
- Incentivise staff to keep their eye on ethics.

The Markkula Center offers a set of tools for use by technology companies to assess ethical risks.[107] These include the following:

1. Ethical "risk sweeps" identify potential risks at regular work intervals to keep ethics principles at the center.
2. "Pre-Mortems" and "Post-Mortems" look for potential "cascade effects" where a series of small or low risk ethical failures can aggregate into an ethical disaster or "systemic design failure."
3. Broad stakeholder analysis that focuses on identifying stakeholders, assumptions about stakeholder positions, and scenario analysis.
4. Practicing case-based analysis so that tech staff have a set of examples in mind when they risk sweep.
5. Highlighting the ethical benefits of a product help to keep the focus of ethics on the potential to do good, not just to avoid harm.
6. "Bad actor" identification attempt to anticipate potential criminal uses of technology.
7. Conducting an ongoing audit of ethical impacts is important to provide feedback to staff on their ability to predict and avoid ethical risks.

Strengths

Ethical frameworks are flexible, so companies may find them easier to use than other frameworks. Because ethics frameworks are not regulations, it may enable companies to use ethics as a guide. The malleability of ethics makes it easier for software engineers and business managers to translate ethical principles into checklists, project management frameworks, coding packages to evaluate algorithmic bias, and learning techniques.[108] An ethics approach can provide the nuance and analysis necessary to operationalise human rights.

Ethical frameworks enable early warning of potential harms. Ethics frameworks offer the types of questions that companies can use at the early stages of product design and development. This can provide insight into potential harms and even anticipate potential violations of human rights or regulation that might occur down the road. Facebook's advertising platform allowed markets to choose which audiences could see their ads. Tech designers may have imagined an ethical user, benignly choosing audiences according to those most likely to be interested in the product. An ethics lens and ethical risk-sweeping exercise might have helped uncover the discrimination stemming from advertising practices or algorithms.[109]

Ethical frameworks may address the harms generated by some companies' profit models. Ethics tools can help to address difficult questions about the tech harms associated with business models by facilitating broader thinking across teams and departments about the various potential impacts of business decisions and product design.

Weaknesses

The informality of many ethical frameworks lacks clarity and consensus. Unlike formalised regulations and human rights codes, ethics frameworks and principles can be ambiguous and may be interpreted differently even within the same company depending on cultural or contextual meanings and understandings. The informality enables companies to ignore or manipulate them toward profit margin calculations. The informality of ethics frameworks may make it easier for companies to ignore obvious harms – such as the Myanmar military's use of Facebook to spread disinformation and propaganda instigating genocidal violence against the Rohingya ethnic group.

Some ethics approaches may offer the "Illusion of Completion." Even if ethics principles are turned into checklists, it may wrongly imply that ethics "has been done." The Markkula ethics framework, in contrast, offers an ongoing everyday set of questions and processes to anticipate and respond to harms, not a one-time checklist. Meaningful ethics are never "completed."[110]

Ethics frameworks lack normative and enforcement power. The sanctions for causing harms not already enshrined in legal or human rights frameworks rely on media attention, public pressure and/or shareholder pressure. Tech companies are investing large sums in lobbying governments to participate in processes of identify regulations, and push for more lax regulations. Companies may be even more reluctant to agree to ethical standards that they did not contribute toward or take part in drafting. Ethics statements may guide the entities that commit to them, but they do not establish a broad governance framework under which all can operate."[111]

Ethics frameworks often lack accountability mechanisms, oversight mechanisms, or reporting requirements, although there are increasingly tools available for companies to self-assess their corporate cultural ethics.[112] Outsiders may not be able to assess how or whether a company is adhering to their ethical principles, hold them accountable in case a violation is revealed, or provide remedy for any negative impacts.[113]

In the absence of regulations, ethics owners articulate a pressure to implement ethics practices that do not negatively affect companies' bottom lines. As a senior leader in a research division explained, this "means that the system that you create has to be something that people feel adds value and is not a massive roadblock that adds no value, because if it is a roadblock that has no value, people literally won't do it, because they don't have to."[114]

Some companies use "ethics washing" within the "Mirage of Self-Regulation." The informality of ethics frameworks has made it appealing to companies who prefer self-regulation to stave off government regulation.[115] The term "ethics" can create a veneer of action, but in truth may be merely an empty gesture. Critics refer to "ethics washing" as simply an attempt to avoid regulation without accountability or consequences for their actions. The non-profit organisation Article 19 argues that "in multiple cases, this has proven to be a strategy of simply buying time to profit from and experiment on societies and people, in dangerous and irreversible ways."[116] Self-regulation of an industry that is known to cause significant harm is unacceptable when there is no institutional or industry

unity or agreement about interpretation, implementation, evaluation, and enforceability of these principles.

Ethics frameworks may not work in a rule-breaking culture. Ethics frameworks may be especially difficult to use in the rule-breaking subculture of Silicon Valley, where locals tout the saying "fail fast, fail often." The informality of ethics frameworks may be particularly vulnerable and weak in a culture where "breaking rules and ignoring guardrails" both encourages and normalises deviance."[117] Some tech ethic experts argue that tech innovation culture itself must change. Some in the "tech for good" culture in Ontario's "Silicon Valley North" argue ethics can only work as a framework when it changes the culture of tech innovation.[118]

Human Security

The concept of human security was first developed in the 1990s at the end of the Cold War to articulate the need to focus on threats to individuals and communities and not just states. Human security frameworks identify the limitations of traditional national security frameworks which were developed primarily to address threats from states to other states.

Human security frameworks are well suited to address digital technology threats in several ways.[119] While the field of cyber-security emphasises national security paradigms and focuses on tech threats to states, the ICT4Peace Foundation in Switzerland argues that "digital human security" identifies threats to individuals, not just states.[120] A "human-centric" approach to cybersecurity would require governments to protect and extend human rights-related laws and guidance to technology businesses headquartered in their jurisdiction.[121] In the case of new contact tracing technologies, for example, Beatriz Botero Arcila argues a "human centric approach to cybersecurity" would raise new ethical questions about deploying such technologies in the Global South.[122] Digital human security might require, for example, a more robust system of computer emergency response teams (CERTs) to address human rights.[123]

There are two important human security frameworks relevant to technology threats.

UN Human Security Approach

UN General Assembly resolution 66/290 states "human security is an approach to assist Member States in identifying and addressing widespread and cross-cutting challenges to the survival, livelihood and dignity of their people." It calls for "people-centered, comprehensive, context-specific and prevention-oriented responses that strengthen the protection and empowerment of all people."

The UN Human Security Unit emphasises that human security requires two mutually reinforcing principles: 1) protection of civilians, and 2) empowerment of civil society. Protection refers to national and international norms, processes and institutions that shield people from critical and pervasive threats and that address insecurities in ways that are systematic not makeshift, comprehensive not compartmentalised, and preventive not

reactive. The concept of "protection of civilians" has tended to emphasise a "top-down" approach, with states having the primary responsibility.

The concept of "empowerment" emphasises people as actors and participants in defining and implementing their vital freedoms. It implies a "bottom-up" approach and it enables people to develop their potential and their resilience to difficult conditions. People who are empowered can become full participants in decision-making processes and demand respect for their dignity when it is violated. An empowered civil society complements government programmes to advance human security as well as holds governments to account for responsive governance. Civil society can mobilise for the security of others by taking actions.

The UN Human Security Unit defines five principles of human security used to foster deeper understanding of unique cultural contexts as well as to plan for prevention of harm.

1. People-centred. It focuses on the safety and protection of individuals, communities, and their global environment. A human security approach empowers local people to assess vulnerabilities and threats and then identify and take part in strategies to build security rather than imposing outside definitions. Strategies to achieve human security are successful in as much as they protect the quantity and quality of life. This is relevant for digital speech threats because human security platforms provide examples of how diverse local civil society stakeholders could meet with government and technology companies to identify threats to human safety.
2. Comprehensive. In practice, human security strategies range from a limited operational "freedom from fear" to a more encompassing structural approach including "freedom from want" and "freedom to live in dignity." This is relevant for digital speech threats because they encompass both physical threats as well as emotional harms and trauma that come from hate and dangerous speech online.
3. Multi-Sectoral. It addresses a range of interdependent global and local threats, insecurities, and vulnerabilities in security, development, and human rights. This is relevant for digital speech threats because distorted information ecosystems sometimes generate disinformation to fuel hate speech and dangerous speech that spills into physical violence.
4. Context-Specific. Local dimensions of global threats are unique and require context-specific assessment and planning. This is relevant for digital speech threats because local civil society are the experts on how digital technologies are being used in unique ways to polarise and foment conflict.
5. Prevention-Oriented. Conflict prevention and peacebuilding strategies aim for sustainable solutions to address. This is relevant for digital speech threats because the goal is not punishing platforms for harms people cause when using their platforms. Rather, the goal of human security guidance to tech companies would be to prevent harms in the first place by listening closely to local civil society and meeting in prevention-oriented human security platforms.

European Union Approach to Human Security

The 2003 Barcelona Report on European Security Capabilities identified human security as the most appropriate conceptual framework for the EU security strategy to augment each

EU member's national security policies. The Madrid Report of the EU's Human Security Study Group identified six principles of a human security approach.[124] These include the primacy of human rights, a bottom-up or people-centred approach with intensive local consultation, and an effective multilateral and regional approach since human security threats cross state borders.

The UN and EU human security principles emphasise ensuring that local civil society can voice their analysis of harms and threats through processes that are multilateral and regionally focused. Unlike other frameworks, human security has been operationalised as a process or platform that creates opportunities for individuals and communities to talk directly to security sector actors, businesses, and government representatives about threats and harms to human security.

For example, in Ghana, Kenya, the Philippines, and elsewhere, human security coordination platforms bring together civil society, the government, and military on a regular basis to identify harms or potential harms to civilians. This process creates a sustainable way to address new threats as they arise without needing to create time consuming one-on-one bilateral processes or address threats on a case-to-case basis. Human security platforms are multi-stakeholder – meaning they include a variety of companies, along with local government and diverse civil society representatives (including youth, women, minority groups, etc.).

Drawing on these models, human security platforms could also empower individuals and communities most impacted by technology in FCS to have a voice directly to technology companies and governments responsible for regulating them. A multistakeholder human security platform can address threats of any kind, including threats from new technologies.

Human security platforms enable stakeholders to build trust and develop more realistic and effective solutions through a variety of processes.[125] A human security platform includes:

- Joint capacity building, to develop a shared language of ethics, with particular attention to regulations, human rights frameworks, conflict sensitivity, and human security principles.
- Joint assessment of human security challenges related to new technology. This could draw on the Markkula Center's tech ethic tools to identify potential harms during the pre-deployment phase. While a broad platform could exist and be used as a forum for multiple tech companies (Facebook, Twitter, Weibo, etc.), individual tech companies could also use the platform as a space to gather feedback and early warning of potential ethical risks in new product development.
- Joint monitoring and evaluation of the implementation or product roll out to gather information from diverse stakeholders on unintended impacts.

A multistakeholder human security platform can also explore potential ways of addressing tech related human security threats and discuss how to manage trade-offs (such as between freedom of speech and extremist recruitment for example). The human security platform delegates roles and implements a multi-sector plan. For example, there might be roles for tech companies in moderating or changing algorithms. Government leaders may issue public information and warnings or create new regulations. Civil society leaders may issue

their own public information campaigns or begin digital peacebuilding initiatives. The platform monitors and evaluates how such measures are working, to learn from what is or is not working.

Strengths

Human security keeps the impacts on people at the forefront of the discussion of digital harms. While the field of cybersecurity typically emphasises state security, human security is "human centric" and therefore puts the safety of individuals and communities at the centre of questions related to ethics, harms, and security.

Human security relies on consultative processes to identify digital risks and digital harms. Human security principles advocate inclusive processes that create opportunities for individuals and communities to have a voice in identifying threats, harms, and benefits. Human security platforms could help to operationalise the consultative elements in the human rights, conflict sensitivity, and tech ethic toolkits to provide opportunities for individuals and communities to voice—and have recourse—on the harms and benefits of technology in their lives.

Human security offers a more comprehensive approach to addressing digital risks and harms that may not be identified in other frameworks. Unlike a human rights framework, the human security approach allows people to articulate how technology harms their individual safety or dignity. It also goes beyond a conflict sensitivity analysis to look at other underlying fragilities communities face. The power to analyse and identify digital risks and harms may not be possible if human rights frameworks do not apply to new forms of technology.

Human security processes are already supported within the UN and EU. The United Nations and European Union both have invested time, infrastructure, and implementation guidance for human security frameworks in FCS. These might be adapted for tech threats in FCS.

Weaknesses

Human security impacts of technology and social media are under-researched. The human security implications of technology and social media is not yet widely researched or understood. There are only a handful of existing articles which link the human security concept to technology threats. Research remains heavily focused on human rights and ethics.

Human security frameworks may not be familiar to tech companies or digital activists in civil society. Human security is relatively unknown within private industry, and among many human rights, conflict sensitivity, or tech ethics practitioners. Some interviewees questioned whether a human security framework was superfluous or could further confuse an already complex field. Human security processes still lack robust field testing of practical guidelines and implementation strategies, unlike conflict sensitivity and human rights.

Analysis and Conclusion

Significant work has already been done and is still underway to determine the impact of certain emerging technologies on societies around the world.

Each framework discussed in this report has its own strengths and weaknesses. Each framework has its own role to play in mitigating the risks of doing business in FCS and also proactively seeking to support peace and human rights. They are mutually reinforcing and align in many respects. Together, they make a powerful combination of principles, tools, and accountability mechanisms for tech companies to apply. These four approaches can be combined to help address different aspects of the challenges faced. Each individual framework alone is insufficient to properly address the risks of technology. Our research also uncovered additional cross-cutting issues, discussed below. This section describes how these different frameworks relate to one another, and how they might be useful in practical tools and techniques for reducing the risk posed by technology and working together to build peace and human security.

The table below provides a high-level view of our findings.

	Strengths	**Weaknesses**
Human Rights	▪ International consensus and wide acceptance as standards. ▪ Comprehensive in substance as well as implementation guidance and tools. ▪ Relatively effective ways of measuring compliance. ▪ Provides foundation for navigating situations where rights conflict.	▪ Not always explicit or relevant to conflict-affected situations. ▪ At times limiting due to focus on attribution of harms and responsibility. ▪ Often does not involve sufficient engagement with communities in practice. ▪ Current practice fails to account for conflict drivers and impacts. ▪ May exclude important considerations. ▪ Sometimes only superficial compliance.
Conflict Sensitivity	▪ Focuses specifically on threats that may amplify potential for violence or inhibit social cohesion and peace processes. ▪ Helps companies understand the broader implication of seemingly neutral business activities. ▪ Fills gaps regarding conflict analysis and can be easily integrated into other analyses and frameworks. ▪ Takes a systemic view of complex situations. ▪ Can highlight trade-offs that might need to be made in evaluating impacts ▪ Calls for proactive action to support peace.	▪ May also create additional friction or contribute to inaction. ▪ It is difficult to know when it should be applied or what constitutes an FCS. ▪ Relatively less known outside of the peacebuilding and development fields ▪ Limited tools and guidance available for tech companies. ▪ Difficult to measure compliance.

	Strengths	Weaknesses
Tech Ethics	▪ Provides broad guidance on evaluating social benefits and social harms. ▪ Enables public conversation to explore the pros and cons of technology. ▪ Delivers more comprehensive ethical guidance to address threats, complex issues, and trade-offs not addressed by human rights norms and laws. ▪ Emphasises keeping the goal of creating social benefits at the centre of workflows. ▪ An ethic-centred culture is more likely to prevent and minimise harms. ▪ Provides early warning of potential negative impacts of processes.	▪ Lack of widespread agreement on ethical tools and processes. ▪ Internal ethical risk sweeping procedures may be culturally subjective to the staff involved rather than broader stakeholders. ▪ Current practice fails to account for conflict drivers and impacts. ▪ Too informal in some cases and may offer an "illusion of completion" or proliferation of ethics washing. ▪ Easily influenced and diluted by profit and other business considerations. ▪ Incompatible with a "rule breaking" culture like that of Silicon Valley. ▪ Difficult to measure compliance.
Human Security	▪ Supported by the UN and EU. ▪ Emphasis on community consultation and involvement in identifying harms and risks ▪ Human centric, putting individuals at the centre of questions related to harms. ▪ Comprehensive and encompassing a broad range of issues.	▪ Relatively less known outside of the peacebuilding and development fields. ▪ Little existing relevant guidance for tech industry. ▪ Difficult to measure compliance.

Cross-Cutting Issues

Several additional issues arose during our consultations and research. They are discussed in turn below.

Industry receptivity. Several stakeholders raised interesting points that impact the potential for companies to adopt and incorporate the different frameworks, as well as their potential practicability. Across the board, our interviews indicated a consistent perception that the tech industry is both the most familiar with and receptive to a human rights framework for mitigating the risks of social media in FCS and generally. Leading business and human rights CSOs have already developed (and in many cases technology companies have already implemented) human rights due diligence tools tailored to the tech industry.[126] Despite efforts from the UN and others to raise awareness about conflict sensitivity and human security processes in and among the private sector, the tech industry has remained relatively unfamiliar with even the more basic principles of a conflict sensitivity and human security frameworks. The industry appears to be quite familiar with ethical frameworks, based on the frequent discussions of ethics principles, ethics boards, and the proliferation of ethical guides in the industry.

Tailoring frameworks to address conflict. Only conflict sensitivity and human security frameworks are specifically tailored to understanding conflict dynamics and the well-being

of communities on a broader scale. Human rights is broadly applicable in conflict settings but does not specifically require companies to understand their role in a conflict and the broader impact of their actions on the conflict or society. For example, a company may take steps to protect certain salient human rights by undertaking actions that exacerbate the conflict and potentially cause additional, unforeseen negative human rights impacts to emerge. However, this gap is closing, as civil society and the United Nations address how to tailor human rights due diligence to regions prone to violent conflict. The 2020 UN Working Group Report on Conflict directly addresses this and explicitly calls for heightened HRDD and a conflict sensitive approach. Tech ethics does not preclude tailoring to conflict-affected situations, but in order to make relevant ethical decisions and conduct ethics sweeping, a company would have to undertake a conflict sensitivity analysis and be informed by human security and human rights concerns.

Practicality and potential for impact. The UNGPs, along with the existing tools for effective human rights due diligence implementation, makes a human rights approach one of the more easily and immediately operationalizable for industry. Conflict sensitivity is complementary to human rights and can be integrated into existing human rights due diligence processes relatively easily. Ethics and human security, similarly, have relatively simple practical implementation. However, whether these frameworks can be put into practice does not necessarily mean that they will be impactful. Some interviewees suggested that for a framework to have impact, it must be enforceable. Human rights is currently the only framework with an existing accountability and enforcement mechanism, although it is currently limited to states. The greatest source of enforcement and accountability for tech and human rights norms likely comes from reputational risk and consumer brand identity.

This poses a challenge for enforcement given that many tech companies are not in fact consumer-facing and therefore may be less motivated to comply with human rights standards they view as voluntary. There have increasingly been moves to codify human rights due diligence requirements in domestic laws across jurisdictions, but these pertain largely to industries with traditional supply chains (e.g., the UK Modern Slavery Act, the French Duty of Vigilance Act). Ethics similarly poses an opportunity for enforcement through reputational risk and consumer brand identity, because being branded as "unethical" resonates with consumers, whether or not there is a clear understanding of the nuances of the ethical issue at hand. Conflict sensitivity and human security offer little, if any, opportunity for enforcement. However, they do offer an opportunity to motivate companies to take positive action – boosting their reputation through "doing good" rather than merely "doing no harm." This increases their potential for making a positive impact, as it moves the issues out of just reducing risks and into the realm of making positive contributions to communities and society.

"Triggers" for these frameworks. Many respondents for this report noted that a significant hurdle for developing responses to conflict is knowing what situations constitute "fragile" or "conflict-affected" settings, and what activity on the ground should trigger enhanced due diligence or responsibilities. Human rights impact assessments are generally conducted when a company enters a new market or releases a new product or service. Despite guidance indicating that they should be ongoing, they rarely are. It is important to know when a tech company, especially a social media platform, should engage with these

frameworks or enhance existing due diligence. With the integration of technology into our everyday lives and the extensive impact on society of social media, this is a challenging question. Few considered the United States to fall into the category of FCS when the January 6 attack on the Capitol Building happened. Sometimes, as in Ethiopia, different regions of a country might be more prone to conflict than others – or there might be multiple, overlapping, and inter-related conflicts, where action to reduce conflict in one region might exacerbate conflict in another. In Myanmar, the tech industry was slowly but steadily improving its human rights practices following the Rohingya genocide when there was a military coup, massively changing the context, stakeholders, and potential inroads for building peace and human security. While there may be special cases that require extra due diligence, all four frameworks should be operationalised in all contexts given the significant digital risks that exist to all communities.

Addressing the complexity of technology and its impacts. Another issue requiring more research is whether all these impacts may be characterised by existing human rights categories. Some of the impacts of technology on society are more nuanced and subtle—such as undermining social cohesion or reinforcing structural inequalities—although these impacts can be as dangerous as direct human rights abuses. Similarly, the phrase "technology" is deceptive and does not reflect the true complexity and extent of the industry. This has very practical implications for this research. For example, do companies need to undergo algorithmic impact assessments as part of human rights and conflict sensitivity impact assessments? Doing so can be difficult. As noted by Data & Society,

> [algorithmic] impact assessment regimes are evolving, power-laden, and highly contested—the capacity of an impact assessment regime to address harms depends in part on the organic, community-directed development of its components. Indeed, in the co-construction of impacts and accountability, what impacts should be measured only becomes visible with the emergence of who is implicated in how accountability relationships are established.[127]

Moreover, applying any of these frameworks requires untangling extremely complex relationships between business partners, supply chains, clients, customers, users, and communities. Addressing issues related to one can have unintended repercussions throughout the system.

Recommendations

Instead of relying just on human rights or "enhanced human rights due diligence," it is necessary for all relevant stakeholders to come together and work toward the synthesis of a comprehensive approach that considers all relevant frameworks: human rights, conflict sensitivity, tech ethics, and human security. All four frameworks can inform tech company policies and practices to ensure that their products and operations do not contribute to or foment violent conflict. However, much progress is required to get there.

By the time human rights practices are improved, conflict sensitivity is implemented, ethical tools are developed and implemented, and companies learn enough about human security processes to start taking positive, proactive action to improve rights and human security, it may be too late for some. There is an urgent need for action, and, for the most part, we have the basic components to do so. However, now it is time to put these frameworks into action.

To do so, we have highlighted the following recommendations for industry, civil society, academia, and donors:

1. **Define what types of indicators related to conflict would trigger enhanced responsibilities**. A significant hurdle for developing responses to at risk countries is knowing what situations constitute "risk" or "fragile" or "conflict-affected" settings, and what activity on the ground should trigger enhanced due diligence or responsibilities.
2. **Understand what "enhanced due diligence" is and would require.** Human rights due diligence has many different components and ranges of activity. At a base level, there is the low-level ongoing due diligence that may include building out internal ethical policies, a human rights policy, and internal capacity building. Then there is more active due diligence, such as legal compliance and impact assessments. Understanding when and how that due diligence should be enhanced once the potential for serious violent conflict is detected is a significant gap. As a practical first step, the companies should begin by incorporating into their existing Human Rights Impact Assessments (HRIAs) certain specific, narrowly tailored questions geared toward ensuring conflict sensitive product design, deployment and use in high-risk settings.
3. **Distinguish between types of impact on conflict.** The tech industry is complex, and various activities can have impacts on conflict dynamics and social cohesion. Whether they relate to protected speech, internet connectivity, algorithmic impacts, or business models, each needs to be analysed as part of a thorough due diligence process.
4. **Create a community of practice and expertise that doesn't just include but elevates stakeholders from local communities.** Understanding conflict contexts, algorithmic harms, human rights harms, and balancing ethical obligations and human security requires a broad community of experts. This includes community advocates and members of impacted groups, historians, sociologists, policy makers, scholars, and technologists, amongst others.

5. **Support community-based and co-created processes for anticipating and analyzing tech impacts and harms and developing appropriate remedy.** It is also critical for developing appropriate peacebuilding initiatives, remedy schemes, or similar. At the same time, the technology industry should try to reduce the burden on affected communities and "engagement burnout" by sharing knowledge, processes, and, when possible, joining together for meaningful engagement opportunities.
6. **Curate a set of case studies that identifies both failures to anticipate harm as well as cases that illustrate good practices.** More examples are needed to identify "paradigm cases" that can help tech companies understand the variety of harms possible as well as the innovations some tech companies are making to avoid and minimise harms.
7. **Offer incentives and a reward structure for technology staff and companies that illustrate best practices in ethics, human rights, conflict sensitivity and human security**, for example, aligning metrics that indicate respect for human rights and conflict sensitivity in the key performance indicators of relevant personnel such that those criteria are considered in the awarding of year-end compensation. While regulations sanction tech company mistakes and harms, reward structures are necessary for incentivising new processes to infuse tech design workflows with these four ethical frameworks.
8. **Look to lessons learned from other sectors for best practices for implementation.** Other industries have adopted strategic responses to conflict in ways that directly and indirectly impact the conflict. For example, direct responses include lobbying the government to resolve the conflict, speaking out publicly against violence, acting as mediators and organising negotiations. Indirect responses have included changing business practices to adhere to multilateral agreements, changing hiring and human resources practices to avoid exacerbating ethnic tensions, making humanitarian donations, or adopting industry codes of conduct for doing business in at risk countries or Fragile and Conflict-Affected Situations (FCS).[128]

Annex

List of Interviewees

1. Paul Barrett, Stern Center for Business & Human Rights
2. Cathy Buerger, Dangerous Speech
3. Steven Feldstein, Democracy, Conflict and Governance Program at Carnegie Endowment for International Peace
4. Tamara Grigoryeva, Creative Associates
5. Lisa Inks, Mercy Corps
6. David Jay, Center for Humane Technology
7. Elizabeth Kariuki, International Alert
8. Dia Kayyali, Mneumonic
9. Ayan Kishore, Creative Associates
10. Michael Kleinman, Amnesty International (participating in his personal capacity)
11. Mark Latonero, Data & Society
12. Rebecca MacKinnon, Wikimedia
13. Nathalie Marechal, Ranking Digital Rights
14. Mary Martin, London School of Economics, IDEAS
15. Brandie Nonnecke, CITRIS Policy Lab at UC Berkeley
16. Charlotte Onslow, International Alert
17. Iria Puyosa, Atlantic Council's Digital Forensic Research Lab
18. Mark Silverman, ICRC
19. Ann Skeet, Markkula Center for Applied Ethics, University of Santa Clara
20. David Sullivan, Digital Trust and Safety Partnership
21. Evelyne Tauschnitz, Lucerne Graduate School in Ethics (LGSE) and Centre for Technology and Global Affairs (CTGA), University of Oxford
22. Jenny Vaughan, Business for Social Responsibility

---

[1] United Nations Human Rights Office of the High Commissioner (2020). Governments and Internet Companies fail to meet challenges of online hate – UN expert, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25174&LangID=E

[2] Defining what a "technology company" is has become increasingly difficult. We are aware that technology companies often use and develop vary diverse technologies, such as using AI to support social media platform performance, for example. Many of the same conclusions we've developed in this report are broadly applicable to different companies and technologies. However, for the sake of clarity and because social media is a pressing issue in FCS, we have focused our analysis on social media and platform companies.

[3] Evelyn Douek, Why Facebook's 'Values' Update Matters, Lawfare.com, 16 September 2019, available at https://www.lawfareblog.com/why-facebooks-values-update-matters.

[4] Theo Dolan, Preventing Media Incitement to Violence in Iraq, USIP Peace Brief, April 7, 2010.

[5] The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze, Case No. ICTR-99-52-T, Appeals Judgement, 28 November 2007.

[6] Lisa Schirch, editor. (2021). Social Media Impacts on Conflict and Democracy: The

Techtonic Shift. Sydney: Routledge Press. 7-9.

[7] Ibid.

[8] Ibid.

[9] See chapters in Social Media Impacts on Conflict and Democracy (2021) by Spandana Singh (India); Diego Casaes and Yasodara Cordova (Brazil); Tendai Marima (Zimbabwe); Brendan McCourt (Northern Ireland); Diana Dajer (Colombia); Iria Puyosa (Venezuela); and Victoire Rio (Myanmar).

[10] Shoshana Zuboff. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.

[11] Tristan Harris. (2019). "Technology is Downgrading Humanity: Let's Reverse That Trend Now." Center for Humane Technology. Medium. July 17.

[12] There are several other ways that technology can increase risks to people in FCS, including exploitation of personal data, digital surveillance, irresponsible use of emerging technologies, and others. Together, these harms are often referred to as "digital risks." ICRC, Digital Harms (2021), 5.

[13] Casey Newton. (2021). "The Tier List: How Facebook Decides Which Countries Need Protection." The Verge. October 25. https://www.theverge.com/22743753/facebook-tier-list-countries-leaked-documents-content-moderation

[14] Lee Haleand Eyder Peralta. (2021). "Social media misinformation stokes a worsening civil war in Ethiopia." National Public Radio. October 15. https://www.npr.org/2021/10/15/1046106922/social-media-misinformation-stokes-a-worsening-civil-war-in-ethiopia

[15] International Alert. (2018). Human Rights Due Diligence in Conflict-Affected Settings, 15, available at https://www.international-alert.org/sites/default/files/Economy_HumanRightsDueDiligenceGuidance_EN_2018.pdf

[16] UN General Assembly, UN A/75/212 (2020). Issue of human rights and transnational corporations and other business enterprises, paras 50-51, available at https://undocs.org/en/A/75/212 (hereinafter UN A/75/212).

[17] See World Bank. (2021). "Classification of Fragile and Conflict-Affected Situations." https://www.worldbank.org/en/topic/fragilityconflictviolence/brief/harmonized-list-of-fragile-situations

[18] UN A/75/212, para 17.

[19] UN A/75/212, para 18.

[20] UN A/75/212, paras 19-21.

[21] UN A/75/212, paras 58 – 71.

[22] Reuters, Facebook will move UK users to US terms, avoiding EU privacy laws, 15 December 2020, https://www.theguardian.com/technology/2020/dec/15/facebook-move-uk-users-california-eu-privacy-laws; Reuters, Exclusive: Google users in UK to lose EU data protection-sources, 19 February 2020, https://www.reuters.com/article/us-google-privacy-eu-exclusive-idUSKBN20D2M3.

[23] See, e.g., UK Modern Slavery Act; US FARS regs on the subject (Section 2(2)(A) of Executive Order 13627). Robert McCorquodale, Lise Smit, Stuart Neely, and Robin Brooks. (2017). Human Rights Due Diligence in Law and Practice: Good Practices and Challenges for Business Enterprises, Business and Human Rights Journal, 2, 195-224, CUP.

[24] Elsa Savourey and Stéphane Brabant. "The French Law on the Duty of Vigilance: Theoretical and Practical Challenges Since Its Adoption." Business and Human Rights Journal 6, no. 1 (2021): 141–52. doi:10.1017/bhj.2020.30.

[25] Amnesty International. (2019). Devoir de Vigilance: Les Entreprises Peuvent Mieux Faire, available at https://www.amnesty.fr/responsabilite-des-entreprises/actualites/les-

entreprises-dans-le-viseur-des-ong; Sherpa. (2021). Creating a Public Authority to Enforce the Duty of Vigilance Law: A Step Backward? Available at https://www.business-humanrights.org/en/latest-news/sherpa-publishes-critical-analysis-on-potential-creation-of-public-authority-to-enforce-french-duty-of-vigilance-law/

[26] See, e.g., House Hearing, 113 Congress (2013), The Unintended Consequences of Dodd-Frank's Conflict Minerals Provision, available at https://www.govinfo.gov/content/pkg/CHRG-113hhrg81758/html/CHRG-113hhrg81758.htm

[27] Whereas this risk tends not to be accounted for in hastily passed legislation that can be clunky and overly broad, the report of the UN Working Group on the application of the UNGPs in FCS refer expressly to and provide guidance for companies' responsible exit in situations of last resort.

[28] See, e.g., House Hearing, 113 Congress.

[29] In establishing the human rights that apply to companies vis-a-vis the UNGPs, the commentary to Principle 12 of the UNGPs states that:

An authoritative list of the core internationally recognised human rights is contained in the International Bill of Human Rights (consisting of the Universal Declaration of Human Rights and the main instruments through which it has been codified: the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights), coupled with the principles concerning fundamental rights in the eight ILO core conventions as set out in the Declaration on Fundamental Principles and Rights at Work.

United Nations Human Rights Office of the High Commissioner. (2011). Guiding Principles on Business and Human Rights, p.13, available at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (hereinafter UN UNGPs).

[30] UN UNGPs.

[31] https://orgs.law.harvard.edu/hub/what-is-bhr/

[32] UN UNGPs.

[33] https://www.paulhastings.com/insights/international-regulatory-enforcement/integrating-human-rights-and-esg-into-international-regulatory-comp-train

[34] UN UNGPs, p.13.

[35] United Nations. UN Resolution A/HRC/38/L.10/Rev.1.

[36] United Nations Human Rights Office of the High Commissioner, Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles – Article 29, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23999&LangID=E

[37] Id.

[38] Id.

[39] BSR. 10 Human Rights Priorities for the Information and Communications Technology Sector, available at https://www.bsr.org/en/our-insights/primers/10-human-rights-priorities-for-the-ict-sector

[40] Id.

[41] UN UNGPs, Principle 13; See also, See, e.g., Debevoise & Plimpton. (2017). Practical Definitions of Cause, Contribute, and Directly Linked to Inform Business Respect for Human Rights, available at https://media.business-humanrights.org/media/documents/files/documents/Debevoise-Enodo-Practical-Meaning-of-Involvement-Draft-2017-02-09.pdf.

[42] John G. Ruggie. (2018). "Facebook in the Rest of the World," John F. Kennedy School of Government, Harvard University, available at, https://media.business-humanrights.org/media/documents/files/documents/John_Ruggie_Facebook_15_Nov_2018.pdf; Mark Latonero and Aina Agarwal. (2021). Human Rights Impact Assessments for AI: Learning from Facebook's Failure in Myanmar, pg. 11.

[43]UN UNGPs, Principle 15

[44] UN Office of the High Commissioner for Human Rights. (2019). UN Human Rights Business and Human Rights in technology Project (B-Tech), Draft Scoping Paper for Consultation, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/B-Tech_Scoping_paper.pdf.

[45] United Nations Human Rights Office of the High Commissioner supra note 1.

[46] Ibid.

[47] United Nations Human Rights Office of the High Commissioner. (2020). B-Tech: Addressing Business Model Related Human Rights Risks: A B-Tech Foundational Paper, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf (hereinafter B-Tech Foundational Paper).

[48] Ibid., pg, 5.

[49] Ibid.

[50] Ibid., pg 7.

[51] UN A/75/212, Para 99.

[52] UN A/75/212.

[53] UN UNGPs, Commentaries to Principles 12 and 23.

[54] UN A/75/212, Para 7.

[55] UN A/75/212, Para 13.

[56] UN UNGPs, Principle 14.

[57] UN A/75/212, Para 52-54.

[58] UN A/75/212, Para 97.

[59] UN A/75/212, Para 99.

[60] UN A/75/212, Para 99.

[61] United Nations Human Rights Office of the High Commissioner. Freedom of Expression vs. incitement to hatred: OHCHR and the Rabat Plan of Action, available at https://www.ohchr.org/en/issues/freedomopinion/articles19-20/pages/index.aspx

[62] Facebook Oversight Board. (2021). Case decision 2021-001-FB-FBR, available at https://www.oversightboard.com/sr/decision/2021/001/pdf-english.

[63] Ibid.

[64] Susan Benesch. (2020). But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies, Yale Journal on Regulation Online Bulletin. 3. https://www.yalejreg.com/bulletin/but-facebooks-not-a-country-how-to-interpret-human-rights-law-for-social-media-companies/

[65] Ibid.

[66] See, e.g., websites of the B-Tech Project and the UN Working Group on business, human rights and conflict-affected regions projects, respectively. Available at https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx#:~:text=The%20B%2DTech%20Project%20provides,UNGPs)%20in%20the%20technology%20space.&text=Focus%20Area%201%3A%20Addressing%20Human,Due%20Diligence%20and%20End%2DUse and https://www.ohchr.org/EN/Issues/Business/Pages/ConflictPostConflict.aspx

[67] Christiaan van Veen and Corinne Cath. (2018). "Artificial Intelligence: What's Human Rights Got To Do With It?", Data&Society Points, available at https://points.datasociety.net/artificial-intelligence-whats-human-rights-got-to-do-with-it-4622ec1566d5

[68] UN UNGPs, Principle 14.

[69] United Nations Human Rights Office of the High Commissioner. (2019). UN Human Rights Business and Human Rights in Technology Project (B-Tech), Overview and Scope, para 43, available at https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Project_revised_scoping_final.pdf

[70] Ibid. para 42.

[71] see Artificial Intelligence & Human Rights: Opportunities & Risks

[72] Mark Latonero. (2020). "AI Principle Proliferation as a Crisis of Legitimacy." Carr Center Discussion Paper Series, 2020-011, pg. 6.

[73] Ibid. pg. 2.

[74] Article 19. (2019). "Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence" pg. 16.

[75] Ibid. pg. 17.

[76] See, e.g., Oxfam America. (2013). Community-Based Human Rights Impact Assessment Initiative, available at https://www.oxfamamerica.org/explore/issues/economic-well-being/private-sector-engagement/community-based-human-rights-impact-assessment-initiative/

[77] See, e.g., Mark Latonero and Aaina Agarwal. (2021). Human Rights Impact Assessments for AI: Learning from Facebook's Failure in Myanmar. Harvard University: Carr Center Discussion Paper Series.

[78] Mark Latonero. (2018). Governing Artificial Intelligence. Data & Society. See also, Latonero and Agarwal supra note 77 at pg. 8.

[79] Latonero and Agarwal supra note 77 at pg. 7.

[80] Ibid. pg. 11.

[81] For an overview of conflict assessment tools and approaches, see Lisa Schirch. (2014). Conflict Assessment and Peacebuilding Planning: Participatory Approaches to Human Security. Boulder, CO: Lynne Rienner Publishers.

[82] See for example Mary Anderson. (1999). Do No Harm: How Aid Can Support Peace - Or War. Boulder, CO: Lynne Rienner Publishers.

[83] SwissPeace. (2012). KOFF conflict sensitivity factsheet, pg. 2.

[84] Andreas Graf and Andrea Iff. (2017). Respecting Human Rights in Conflict Regions: How to Avoid the 'Conflict Spiral. Business and Human Rights Journal 2 (2017) 109. Available at https://www.swisspeace.ch/assets/publications/downloads/Articles/98940daeaa/Respecting-Human-Rights-in-Conflict-Regions-17-swisspeace-andrea_iff-andreas_graf.pdf

[85] UN Global Compact. (2002). Global Compact Business Guide for Conflict Impact Assessment and Risk Management, available at https://www.unglobalcompact.org/docs/issues_doc/Peace_and_Business/BusinessGuide.pdf

[86] Ibid.

[87] JustPeace Labs. (2020). Technology in Conflict, pg. 14. Available at https://justpeacelabs.org/.

[88] International Alert. (2018). Human Rights Due Diligence in Conflict-Affected Settings, pg. 23. Available at https://www.international-alert.org/sites/default/files/Economy_HumanRightsDueDiligenceGuidance_EN_2018.pdf

[89] Graf and Iff, pg. 120 - 121.

[90] International Alert, pg. 8.

[91] International Alert, pg. 14.

[92] UN UNGPs, Commentary to Guiding Principle 7.

[93] Graf and Iff, pg. 114.

[94] UNGPs, Principle 7.

[95] Graf and Iff, pg. 121.

[96] International Alert, pg. 14.

[97] Graf and Iff, pg. 132.

[98] Graf and Iff, pg. 132.

[99] For more information on other definitional approaches to ethics, see, e.g., the Stanford Encyclopedia of Philosophy. (2016). Virtue Ethics. Available at https://plato.stanford.edu/entries/ethics-virtue/.

[100] Renieris, Elizabeth. (2021). "Starting Now on Tech Ethics." Me, Myself, and AI. Found on MIT Sloan Management Review. June 22.

[101] Jacob Metcalf, Emanuel Moss, and danah boyd. (2019). "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics." Social Research: An International Quarterly, Volume 82, Issue 2, Summer, pp. 449-476.

[102] Reid Blackman. (2020). "A Practical Guide to Building Ethical AI." Harvard Business Review. October 15.

[103] Shannon Vallor, Brian Green, and Irina Raicu. (2018). "Ethics in Technology Practice: A Toolkit." The Markkula Center for Applied Ethics at Santa Clara University. P. 5.

[104] Shannon Vallor, Brian Green; Irina Raicu. (2018). "Tech Ethics: Best Practices." Markkula Center for Applied Ethics at Santa Clara University.

[105] Ibid., pg. 2.

[106] Ibid., pg. 4.

[107] Shannon Vallor, Brian Green, and Irina Raicu. (2018). "Ethics in Technology Practice: A Toolkit." The Markkula Center for Applied Ethics at Santa Clara University.

[108] Metcalf, et al, p. 4, 10.

[109] Pema Levy. (2019). "Facebook is Cracking Down on Ad Discrimination. But the Bias May Be Embedded in Its Own Algorithms, Mother Jones, 12 July. https://www.motherjones.com/politics/2019/07/facebook-is-cracking-down-on-ad-discrimination-but-the-bias-may-be-embedded-in-its-own-algorithms/

[110] Metcalf, et al, p. 10.

[111] Eileen Donahoe, and Megan MacDuffee Metzger. "Artificial Intelligence and Human Rights." Journal of Democracy, Volume 30, Number 2, April 2019, pg. 118, (pp. 115-126.)

[112] See, e.g., Markkula Center for Applied Ethics, Culture Self-Assessment Practice, available at https://www.scu.edu/ethics/culture-assessment-practice/.

[113] Article 19. (2019) "Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence." April 17. P. 9.

[114] Metcalf, et al, P. 8.

[115] Metcalf, et al, P. 7.

[116] Article 19, P 10.

[117] Metcalf, et al, p. 10.

[118] Paul C. Heidebrecht. (2021). "Peacebuilding and the Norms of Technological Change." Tokyo: Toda Peace Institute. February. https://toda.org/assets/files/resources/policy-briefs/t-pb-103_peacebuilding-and-norms-of-tech-change_heidebrecht.pdf

[119]See: Julie Shannon and Nick Thomas. (2005). "Human Security and Cyber-Security: Operationalizing a Policy Framework." In Cyber-Crime: The Challenges in Asia. Edited by Roderic Broadhurst and Peter Grabosky. Aberdeen, Hong Kong: Hong Kong University Press. Pp. 327-346. Emmanuel Darmois and Geneviève Schméder. (2016). "Cybersecurity: a case for a European approach." European Union Human Security Study Group.

[120] Barbara Weekes and Daniel Stauffacher. (2018). "Digital Human Security 2020." ICT4Peace Zurich and the Hub for Ethics and Technology.

[121] Ronald J. Deibert, (2018). "Toward a Human-Centric Approach to Cybersecurity." Ethics and International Affairs. 32, no. 4. Pp. 411-424.

[122] Beatriz Botero Arcila. (2020). "A Human Centric Framework to Evaluate the Risks Raised by Contact-Tracing Applications." ICT4Peace Foundation, Geneva. April 22.

[123] Deibert; 420.

[124] Study Group on European Security Capabilities. (2007). "A European Way of Security. The Madrid Report on the Human Security Study Group." https://www2.world-governance.org/article78.html?lang=en

[125] Lisa Schirch with Deborah Mancini-Griffoli. (2015). Local Ownership in Security: Case Studies of Peacebuilding Approaches. The Hague, The Netherlands: Alliance for Peacebuilding, GPPAC, University of Notre Dame Kroc Institute.

[126] Lindsey Anderson and Joanna Lovatt. (2021). Human Rights Due Diligence of Products and Services. BSR; Danish Institute for Human Rights (2019). Human Rights Impact Assessment of Digital Activities, Danish Institute for Human Rights.

[127] Emanuel Moss, Elizabeth Anne Watkins, and others. (2021). Assembling Accountabiliyt: Algorithmic Impact Assessment for The Public Interest. Data & Society, pg. 7.

[128] UN Global Compact. (2010). Doing Business While Advancing Peace and Development, pg. 10. Available at https://www.unglobalcompact.org/docs/issues_doc/Peace_and_Business/DBWAPD_2010.pdf

The Authors

Jennifer Easterday is Jennifer is Co-Founder and Executive Director of JustPeace Labs. She is a technology and human rights specialist and an attorney with expertise in human rights law, international criminal law, transitional justice and peacebuilding. As a practitioner, her work with NGOs and international tribunals focuses on strengthening international responses to armed conflict and mass human rights abuses. Her work with the private sector focuses on helping companies develop and implement human rights due diligence and conflict sensitivity procedures, with a focus on the intersection of technology, human rights, and conflict. Jennifer has consulted for a variety of non-profit organizations, including the Digital Freedom Fund, Open Society Justice Initiative, BSR, and International Criminal Law Services. She has a J.D. from UC Berkeley, and is in the final stages of a PhD in Law from the University of Leiden. Jennifer has published numerous chapters, articles, and is an editor of two volumes on Jus Post Bellum.

Hana Ivanhoe is Strategy Director of JustPeace Labs. Ivanhoe is an attorney with over 12 years of policy research and advocacy expertise in business and human rights and corporate responsibility. Ivanhoe is currently a consultant for JustPeace Labs and other leading nonprofit organizations, including Oxfam America and Business for Social Responsibility. She is also a lecturer at Berkeley Law (University of California, Berkeley), where she teaches corporate Anticorruption Compliance. At JustPeace Labs, her work focuses on industry engagement around conflict sensitive approaches to responsible technology. Ivanhoe has a Juris Doctor from the University of California, Berkeley School of Law and a Bachelor of Arts from the University of California, Berkeley. Her most recent publication, entitled Combating Corruption to Counter Conflict: Proposals for In-country Reform and International Community Intervention, was published in the Berkeley Journal of Law at the end of last year.

Lisa Schirch is Professor of the Practice of Peacebuilding and the Starmann Chair in Peace Studies at the University of Notre Dame's Kroc Institute for International Peace Studies. She also directs the Socl Media, Technology, and Peacebuilding programme for the Toda Peace Institute. A former Fulbright Fellow in East and West Africa, Schirch is the author of eleven books, including Social Media Impacts on Conflict and Democracy: The Tech-tonic Shift.

JustPeace Labs

JustPeace Labs (JPL), a women-founded and lead 501(c)(3) organisation, advocates for and supports the responsible use and deployment of emerging technologies in high-risk settings – communities experiencing conflict, transitioning from conflict or enduring system human rights abuses.

Contact Us
Email: info@justpeacelabs.org
Twitter: @justpeacelabs

Toda Peace Institute

The **Toda Peace Institute** is an independent, nonpartisan institute committed to advancing a more just and peaceful world through policy-oriented peace research and practice. The Institute commissions evidence-based research, convenes multi-track and multi-disciplinary problem-solving workshops and seminars, and promotes dialogue across ethnic, cultural, religious and political divides. It catalyses practical, policy-oriented conversations between theoretical experts, practitioners, policymakers and civil society leaders in order to discern innovative and creative solutions to the major problems confronting the world in the twenty-first century (see www.toda.org for more information).

Contact Us
Toda Peace Institute
Samon Eleven Bldg. 5th Floor
3-1 Samon-cho, Shinjuku-ku, Tokyo 160-0017, Japan
Email: contact@toda.org

Sign up for the Toda Peace Institute mailing list:
https://toda.org/policy-briefs-and-resources/email-newsletter.html

Connect with us on the following media.
YouTube:@todapeaceinstitute3917
Twitter: https://twitter.com/TodaInstitute
Facebook: https://www.facebook.com/TodaInstitute/