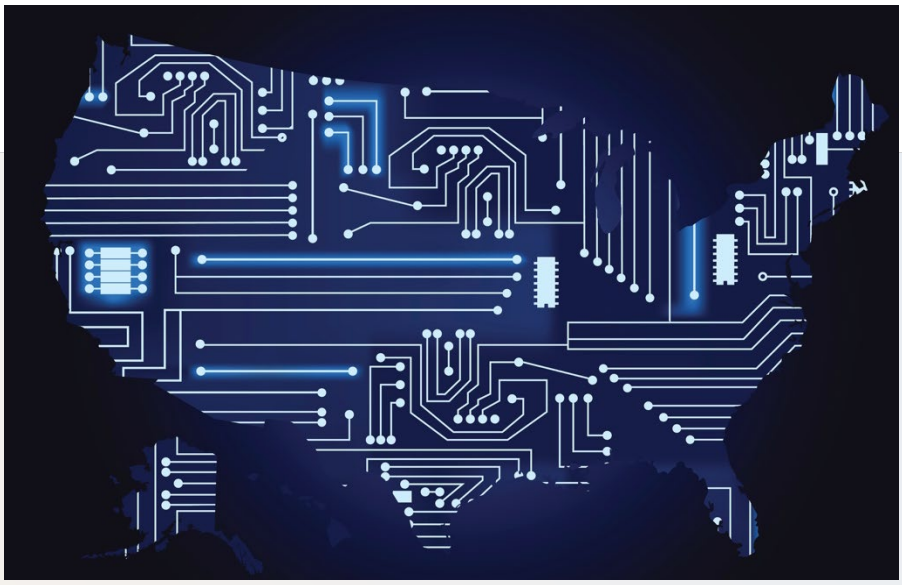


A Human Rights Impact Assessment of Microsoft's Enterprise Cloud and AI Technologies Licensed to U.S. Law Enforcement Agencies

FOLEY HOAG

June 2023

About the Assessors

Members of the Global Business & Human Rights ("GBHR") Practice of the law firm Foley Hoag LLP conducted this Human Rights Impact Assessment ("HRIA.") Launched in 2000, the GBHR Practice completed the world's first HRIA, assisted Professor John Ruggie in drafting the U.N. Guiding Principles on Business and Human Rights, and continues to provide counsel regarding human rights challenges and leadership for multiple industries across six continents.

The Practice conducts human rights monitoring and risk assessments for the banking, extractive, information and communication technology, manufacturing, private equity, and retail sectors to integrate respect for internationally recognized rights into management practices and supply chains. Practice group members are actively engaged in multi-stakeholder initiatives and have served as Assessors for the Global Network Initiative, as the Secretariat of the Voluntary Principles on Security and Human Rights, and as Legal Counsel to the Nuclear Power Plant & Exporters Principles of Conduct.

Team members for this Assessment included Practice Chair, Gare A. Smith; Privacy and Data Security Co-Chair, Christopher Hart; Senior Advisor, Isa Mirza; Associate, Rumbidzai Maweni; and consultant Akshay Walia.

Table of Contents

responsibility Microsoft might have for downstream adverse human rights impacts, such as discriminatory policing, surveillance, and incarceration. The precise degree of Microsoft's responsibility, however, is unclear under the UNGPs.

3. In a few cases, Microsoft is actively involved in developing products, such as for the New York Police Department, through the company's consulting services. In those cases, the relationship between Microsoft and any downstream adverse impact is more concrete, and Microsoft has at least the responsibility to mitigate impacts.

4. Although Microsoft's human rights policies and practices are robust, civil society groups, particularly representatives of the human rights community, perceive a lack of transparency with respect to product design and deployment. This hinders Microsoft's ability to speak with authority on human rights issues.

C. Priority Recommendations

Foley Hoag offers a number of recommendations to Microsoft. Among the most important are the following.

1. Notwithstanding interpretations of law or the UNGPs, as a best practice Microsoft should contribute to efforts to address downstream adverse human rights impacts even when it is solely providing platforms, and seek to mitigate potential adverse impacts in such circumstances. The Assessors note that Microsoft has already proactively been taking such actions through its internal human rights policies and practices and its due diligence efforts.

2. As a best practice, Microsoft should consider assuming some responsibility to remediate actual harms when it has provided consulting services to help develop cloud and AI products for domestic law and immigration enforcement agencies.

3. Microsoft should increase transparency, in particular by proactively seeking input from civil society with respect to its product design, deployment, and impact.

4. Microsoft should find ways to strengthen the work and reach of its internal human rights team throughout the company.

5. Microsoft should emphasize its expectation through its bespoke contracts, terms of service, and other related documents that its counterparties, customers, and partners will respect human rights when using Microsoft products.

6. Microsoft should continue to expand and explore additional ways to use its technology, consulting services, public advocacy, and lobbying to mitigate the potential for downstream abusive conduct by law and immigration enforcement personnel.

II. Introduction

Members of the Global Business and Human Rights Practice at the law firm Foley Hoag conducted this HRIA between March 2022 and April 2023. The Assessment considers how the enterprise cloud services and AI technologies that Microsoft licenses to local and federal U.S. law and immigration enforcement agencies impact the human rights of vulnerable communities in the United States, both beneficially and detrimentally, and how Microsoft might mitigate impacts stemming from the use of those technologies that are adverse.

Microsoft commissioned the HRIA to (1) better understand how rights-holders are impacted by the use of its products in the context of its public-facing human rights commitments, and (2) secure guidance on ways to mitigate any harmful impacts. The Assessment was commissioned in response to a shareholder resolution that was to be considered at Microsoft's November 2021 Annual Shareholders' Meeting.

The resolution requested that Microsoft retain an independent expert to assess how Microsoft's products might be responsible for salient adverse human rights impacts to individuals who identify as BIPOC. The shareholders asked that the independent assessment include mitigating steps Microsoft could take to address such harms.[1] The shareholders withdrew the resolution after Microsoft committed to this Assessment.[2]

Although Microsoft funded the Assessment, Foley Hoag retained independence with respect to research, consultations with stakeholders, and the Assessment's content.

The Assessment provides recommendations to assist Microsoft in mitigating adverse human rights impacts that may be connected to its enterprise cloud services and AI technologies.

III. Background

Microsoft commissioned this HRIA in a political and cultural environment in which individuals and institutions are increasingly aware of the ubiquity of racial discrimination and other serious violations of rights by U.S. law enforcement.

After receiving the proposed shareholder resolution, Microsoft sought to understand what responsibility it might have for any adverse human impacts relating to domestic law enforcement and immigration activities, and how it might best mitigate or remediate such harms. As Microsoft announced in October 2021:

[1] "Microsoft Human Rights Policy Implementation Proposal," *Investor Advocates for Social Justice* (Lead Filer), June 2022.

[2] Ibid.

> In advance of the Microsoft Annual Shareholder Meeting on November 30, we received a request to explore how Microsoft products licensed to public sector entities are experienced by third parties, especially Black, Indigenous and People of Color (BIPOC) and other vulnerable communities. We agree this is a question that warrants greater attention and are contracting an independent third-party to help us identify, understand, assess, and address actual or potential human rights impacts of our products and services.
>
> In conducting investigations like this, we are guided by the UN Guiding Principles on Business and Human Rights (UNGPs). In particular, UNGP Principle 18 notes the value of drawing on external human rights expertise and the importance of meaningful consultation with affected groups and other relevant stakeholders. That will be our approach to this work: We will task the independent third party to engage an expansive audience, with particular focus on […] BIPOC and other vulnerable communities.[3]

The Assessors recognize the vital role that technology plays in all aspects of daily life—and thus the vital role that technology providers such as Microsoft have in delivering those technologies and innovating further. Specifically, Microsoft technologies allow for documents such as this to be written, edited, stored, and shared. They allow businesses to maintain complex data management and communications systems. They are used by institutions as diverse as critical infrastructure providers, hospitals, sports teams, small businesses, government agencies, schools, and manufacturing plants. It is easy to take for granted how much the day-to-day work of contemporary life is made possible, and sometimes even seems seamless, because of the role played by complex digital technology.

Central to this HRIA, it is also essential to recognize the important and legitimate role that domestic law enforcement and immigration authorities play in achieving U.S. objectives for public safety and national security. Microsoft's licensing of digital technologies to relevant agencies can be instrumental in ensuring that these goals are pursued in a manner that is responsible, equitable, and mindful of human rights challenges facing marginalized communities.

Many of the most essential law enforcement activities, however, have led to serious violations of the human rights of BIPOC individuals. Such violations include disproportionate policing, stopping, and detainment of predominately BIPOC individuals (often referred to as "racial profiling"), and subsequent violence to which BIPOC individuals are more subject as a corollary of the activities.[4] Unarmed Black and Latino men are the group most likely to fall

---

[3] "Taking on Human Rights Due Diligence," *Microsoft on the Issues Blog,* October 2020.

[4] "Police Misconduct, Such as Falsifying Evidence, is a Leading Cause of Wrongful Convictions, Study Finds, *USA Today*, September 15 2020; "Government Misconduct and Convicting the Innocent," *National Registry of Exonerations*, September 2020; "Baltimore Police Officer Indicted for Tampering with Evidence," *CNN*, January 25, 2018.

victim to serious police brutality in the United States, including lethal shootings with dubious legal justifications. There is also evidence that police officers may collude to falsify reports and tamper with evidence to avoid heightened public scrutiny when a Black or Latino suspect is injured or killed by police.[5]

Similarly, serious harms are exacted on BIPOC immigrants through immigration enforcement agencies. These harms are systemic: they exist in society writ large and are present across a number of public and private institutions. BIPOC groups – primarily those entering into the United States from the Middle East, North Africa, Central and South America, and the Caribbean — are the most likely to be the target of discriminatory surveillance, arrest, and incarceration by immigration authorities.[6] This includes enforcement actions that lead to the detention and/or deportation of BIPOC immigrants without due process, separation and detention of immigrant children from their families, aggressive home raids on suspected illegal immigrants, and disproportionate use of force or otherwise abusive enforcement practices in securing the U.S-Mexico border.

Advanced technologies, such as AI, present the danger of not only enabling abuses, but of exacerbating them. As Microsoft's Vice Chair and President Brad Smith observed,

> There are many governmental uses of facial-recognition technology that protect public safety and promote better services for the public without raising [multiple concerns]. But when combined with ubiquitous cameras and massive computing power and storage in the cloud, facial-recognition technology could be used by a government to enable continuous surveillance of specific individuals. It could do this at any time or even all the time. The use of such technology in this way could unleash mass surveillance on an unprecedented scale.[7]

In response to these well-known dangers, Microsoft has made numerous concerted, good faith efforts to prevent its technologies from being misused in a way that harms rights-holders. Those efforts include banning the licensing of facial recognition technologies to U.S. police and instituting a robust internal "Responsible AI" program. Microsoft has also used its formidable market presence and reputation to influence policymaking and discussions through its public statements on discriminatory policing and surveillance, and the company's promotion of responsible, inclusive technologies.

This HRIA finds that more can be done. It is not intended, however, to solve the problems of systemic racism in policing and law enforcement. Systemic harms by definition are not caused by any single actor, nor can they be resolved through the actions of a single actor. Rather, the HRIA takes a focused look at specific technologies created and provided by Microsoft that could be, and likely have already been, abused by law enforcement to carry out

---

[5] Ibid.

[6] "Department of Homeland Security Must Stop Targeting Communities of Color," *Brennan Center for Justice*, April 2022.

[7] "Tools and Weapons: The Promise and Peril of the Digital Age," *Brad Smith and Carol Ann Browne*, page 259.

and exacerbate the adverse human rights impacts identified here. By focusing on these specific technologies, the Assessors intend to identify the most salient ways in which Microsoft's products might be related to such harms, and recommend ways that Microsoft can mitigate those harms.

IV. Methodology

A. Scope

The HRIA assesses how, if at all, Microsoft's enterprise cloud services and AI technologies may adversely impact rights-holders in the United States when those services and technologies are used by U.S. law enforcement and immigration authorities.

With respect to affected rights-holders, the Assessment gives particular consideration to the historical and persistent vulnerabilities that disproportionately deprive BIPOC communities in the United States of their rights, and the role of Microsoft's products in benefiting or harming such groups. The HRIA also acknowledges that some BIPOC communities may be at even greater risk of harms if their identities intersect with other historically marginalized characteristics, including being female, children, LGBTQI, people with disabilities or mental illness, and/or recent immigrants.

B. Process

To collect data and first-hand stakeholder perspectives, the Assessment followed a two-pronged research process. First, the Assessors undertook a literature review of Microsoft's key policies, applicable international human rights frameworks to which the policies should adhere, and external reporting and analysis. The Assessors then convened interviews with Microsoft's executive leadership and a range of external stakeholders: academics, legal and public policy experts, human rights organizations, and socially responsible investment firms. The consultation process also included a three-day visit to the company's headquarters in Redmond, Washington to gain an in-depth perspective from its senior executives.

The Assessors spoke with human rights organizations, advocacy organizations specializing in privacy and other digital rights, racial justice and immigrant rights groups, public policy and legal experts, academics, and former officials at key U.S. federal agencies who have first-hand expertise regarding government agencies' use of digital technologies in the provision of public services. In addition, the Assessors interviewed executives at Microsoft responsible for human rights policies and their implementation in the development and sale of technology products to government agencies.

In total, the Assessors held interviews that gathered the perspectives of more than fifty individuals. Interviews were conducted with external stakeholders representing thirty-five organizations from the aforementioned backgrounds, as well as eleven senior executives in Microsoft's Corporate, External, and Legal Affairs ("CELA") Team, including the Office of Responsible AI, U.S. Government Affairs Team, and Racial Equity Initiative.

To protect identities and encourage candor, the Assessors committed to anonymizing and aggregating the feedback cited in the HRIA to the greatest extent possible. At the same time, representatives of civil society and Microsoft's senior executives both emphasized the need for more information sharing related to the impacts of the company's products on rights-holders, disclosure of due diligence results, and conversations regarding human rights challenges in the provision of these products to governments.

Accordingly, the Assessors asked civil society interviewees for permission to list the names of their respective organizations in the HRIA. The intention behind this was to help Microsoft enhance and tailor its stakeholder engagement strategy, including through in-depth discussions regarding specific human rights challenges, information-sharing, and other ways of collaborating with the organizations that participated in the HRIA. Most of the interviewees agreed to provide their organizations' names for the HRIA, with the understanding that doing so did not constitute their endorsement of the Assessment. These organizations are listed in Annex A.

C. Issues Excluded from the HRIA

As Microsoft announced,

> We also want to be clear that this is not a review of all the specific contracts we have in place today, nor is it a broader statement that goes beyond…where, when and with whom we do business. It's also not a blanket prohibition on providing technology across the public sector, as we sell numerous solutions to many public sector customers around the world, and will continue to do so.[8]

With this in mind, the Assessors explain below why certain issues were deemed outside the HRIA's scope.

1. Business Relationships with the Military

The shareholder resolution that prompted this HRIA references several examples of Microsoft's contracts and relationships with the U.S. Department of Defense and other entities that fall within the ambit of the U.S. military. [9] Accordingly, the shareholders expressed an interest in having the HRIA encompass sales to all government agencies, both civilian and military.

Microsoft expressed concern, however, that an HRIA encompassing both military and civilian dimensions could be too broad in scope. Microsoft's senior executives stated that they agreed with the shareholder resolution's overarching objective of focusing on the ways BIPOC communities may have been or could be harmed by the company's products but added that it would be difficult to give this subject the nuanced treatment it deserves if the Assessment also covered Microsoft's commercial contracts with the U.S. military. In particular, Microsoft

[8] Taking on Human Rights Due Diligence," *Microsoft on the Issues Blog,* October 2020.

[9] *See* "Microsoft Human Rights Policy Implementation Proposal," *Investor Advocates for Social Justice* (Lead Filer), June 2022.

executives underscored that the company's relationship with military agencies creates additional layers of complexity, relating to both distinct regulatory requirements and specialized technical features of products designed for military applications.

The Assessors discussed the exclusion of military contracts with approximately twenty representatives of civil society organizations involved in the development of the shareholder resolution. Many of those civil society representatives voiced disappointment over the decision to exclude military uses, emphasizing that a review of these contracts was expressly called for in the shareholder resolution.

Several representatives provided similar views during subsequent one-on-one interviews, opining that the military's use of Microsoft products is intertwined with uses by civilian authorities. Others noted that Microsoft appears to have significant contracts with the U.S. military, and that the products it provides in military settings stand at substantial risk of furthering serious human rights violations through their potential use by foreign governments to commit atrocities, genocide, and other crimes against humanity.

2. Specific Contracts

The Assessors did not review specific contracts between the company and U.S. Government agencies. Microsoft's commercial contracts contain highly sensitive content, including information about Microsoft that the company deems proprietary, and information that the contracting client may view as confidential. Microsoft has a large number of contracts with government entities that the Assessors understand typically contain distinct licensing terms and conditions. Even if a contract review were to be methodologically practicable, an adequate assessment of their various features and particular impacts on rights would be infeasible under this HRIA.

Instead, this Assessment considers opportunities for Microsoft to share more details with civil society and other stakeholders about product licensing to government agencies. Additionally, the Assessors urge Microsoft to strengthen human rights provisions in the contractual terms governing product use.

During the course of interviews, certain members of civil society expressed disappointment with this exclusion. Rights advocates in general regard these limitations as symptomatic of the power they believe technology companies hold in society. Stakeholders made clear that civil society groups want greater transparency and knowledge sharing with respect to the technologies Microsoft licenses to domestic law and immigration enforcement agencies.

V. Applicable International Human Rights Frameworks

A. The United Nations Guiding Principles on Business and Human Rights

The UNGPs are a set of thirty-one principles endorsed in 2011 by the United Nations Human Rights Council.[10] These principles provide the methodological basis for the analysis in this HRIA. The Assessors drew additional direction from the assurance and implementation guidances that form the supplementary UNGPs Reporting Framework.[11]

Microsoft's Human Rights Statement invokes the UNGPs, noting:

> Starting with our initial product design and development, to supply chain manufacturing and management, and finally deployment - we work to identify and understand positive and adverse human rights impacts.
>
> To help us manage these efforts Microsoft commits to respecting the . . . [UNGPs]. We work every day to implement the UNGPs throughout Microsoft, both at headquarters and offices in approximately 200 countries and territories, and throughout our global supply chains.
>
> The UNGPs call upon businesses to respect human rights by conducting due diligence of how their activities might adversely affect human rights, to minimize adverse impacts, and to remediate harms. We communicate our commitment to stakeholders through this Global Human Rights Statement webpage where this statement is available in 18 languages and dialects.[12]

Microsoft's Human Rights Statement further provides that:

> Understanding potential human rights impacts associated with digital technologies presents unique challenges. Our global and on-going processes begin with a focus on identifying and assessing any actual, or potential, adverse human rights impacts that we may cause, contribute or be directly linked with, either through our own activities or as a result of our business relationships. Our processes follows [sic] the UNGPs and the OECD Guidelines for Multinational Enterprises. One of the ways we do this is by conducting [HRIAs], to identify and prioritize salient risks. We have conducted HRIAs at both the corporate and product levels, and for various countries and locations. Our HRIA work includes regular engagement and consultation with stakeholders in an effort to understand and address perspectives of vulnerable groups or populations.[13]

---

[10] "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect, and Remedy' Framework," *United Nations Human Rights Office of the High Commissioner*, January 2011; Also *see* "Launch of John Ruggie's 'Just Business: Multinational Corporations and Human Rights," (Video), NYU School of Law's Center for Human Rights and Global Justice.

[11] *See* "UNGPs Reporting Framework," *Shift* and *Mazars LLP*, February 2015.

[12] Microsoft Global Human Rights Statement, *Microsoft.*

[13] Ibid.

Although the UNGPs are important to Microsoft's human rights due diligence, and inform the analysis in this HRIA, the UNGPs are not a source of law. Accordingly, they should not "be read as creating new international law obligations."[14] They do serve, however, as a framework for businesses to "respect human rights."[15] As Principle 11 underscores, businesses therefore "should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."[16]

Inasmuch as the principles focus on the "corporate responsibility" to "respect human rights," the UNGPs speak in broad terms. "Because business enterprises can have an impact on virtually the entire spectrum of internationally recognized human rights, their responsibility to respect applies to all such rights."[17] However, "some human rights may be at greater risk than others in particular industries or contexts, and therefore will be the focus of heightened attention."[18] From the Assessor's perspective, this means that any particular due diligence exercise may have a different focus depending on the risks involved.

The UNGPs provide that the "responsibility to protect human rights" places a "require[ment]" on businesses. They must "[a]void causing or contributing to adverse human rights impacts through their own activities," "address such impacts when they occur," and "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their" business activities.[19] Thus, businesses "may be involved with adverse human rights impacts either through their own activities or as a result of their business relationships with other parties." The "means through which a business enterprise meets its responsibility" will be "proportional to, among other factors, its size."[20]

When a business "causes or may cause an adverse human rights impact, it should take the necessary steps to cease or prevent the impact."[21] When it instead "contributes or may contribute to an adverse human rights impact," the business "should take the necessary steps to cease or prevent its contribution and use its leverage to mitigate any remaining impact to the greatest extent possible." When an adverse human rights impact is "directly linked" to a business's operations without cause or contribution, "the situation is more complex," and a broad spectrum of context-dependent options may be available to "mitigate the impact."

In addition, if a company "causes" or "contributes" to actual adverse human rights impacts, it "should provide for or cooperate in their remediation through legitimate processes."[22] If it does not cause or contribute, but is directly linked to harm—even actual harm—"the responsibility to respect human rights does not require that the enterprise itself provide for

---

[14] "General Principles," *UNGPs.*

[15] "Principle 11," *UNGPs.*

[16] Ibid.

[17] "Principle 12: Commentary," *UNGPs.*

[18] Ibid.

[19] "Principle 13," *UNGPs.*

[20] "Principle 14: Commentary, *UNGPs.*

[21] "Principle 19: Commentary," *UNGPs.*

[22] "Principle 22," *UNGPs.*

remediation."[23] In those situations, businesses should "[s]eek to prevent or mitigate" such impacts.[24]

The purpose of carrying out human rights due diligence, such as through this HRIA, is to "identify, prevent, mitigate, and account for" how businesses "address their adverse human rights impacts."[25] "The process should include assessing actual and potential human rights impacts." While "actual impacts . . . should be a subject for remediation," "[p]otential impacts should be addressed through prevention or mitigation."[26] To carry this out, the diligence process should "identify and assess the nature of the actual and potential adverse human rights impact with which a business enterprise may be involved."[27]

B. The Universal Declaration of Human Rights

The UNGPs refer to a number of "core internationally recognized human rights" as the "benchmarks against which other social actors assess the human rights impacts of business enterprises."[28] Among these are the Universal Declaration of Human Rights[29] ("UDHR"), the principal doctrine of the U.N. International Bill of Rights. The UDHR articulates the rights to which all individuals are inalienably entitled, regardless of their background and status in society or any other characteristics that define their identity. The two other instruments in the International Bill of Rights, the International Covenant on Civil and Political Rights[30] ("ICCPR") and the International Covenant on Economic, Social, and Cultural Rights[31] ("ICESCR"), expand on certain rights in the UDHR.

For the purposes of this HRIA, the Assessors treat the UDHR as the primary document outlining the fundamental rights that companies are expected to respect in the course of their activities. Few, if any, of the human rights prescribed in the UDHR are independent of one another, and instead intersect and effect each other in multiple ways.

The following UDHR Articles are most pertinent to the scope of this HRIA:

- **Articles 1 & 2 (Right to Equality & Freedom from Discrimination)** – All individuals are born free and equal in dignity and rights. As such, they are afforded

[23] "Principle 22: Commentary," *UNGPs.*

[24] "Principle 13," *UNGPs.*

[25] "Principle 17," *UNGPs.*

[26] "Principle 17: Commentary," *UNGPs.*

[27] "Principles 18: Commentary," *UNGPs.*

[28] "Principle 12: Commentary," *UNGPs.*

[29] *See:* "The International Bill of Human Rights," *U.N. General Assembly Resolution 217 A(III)*, December 10, 1948.

[30] "International Covenant on Civil and Political Rights", adopted and opened for signature, ratification and accession by U.N. General Assembly Resolution 2200 A(XXI), December 16, 1966 and entered into force on March 23, 1976, *See:* pp. 17-34 of the International Bill of Human Rights.

[31] "The International Covenant on Economic, Social and Cultural Rights," adopted and opened for signature, ratification and accession by U.N. General Assembly Resolution 2200 A(XXI), December 16, 1966 and entered into force on January 3, 1976; *See:* pp. 7-16 of the International Bill of Human Rights.

the same set of human rights, regardless of any other identifying characteristic or social status.

- **Article 3 (Right to Life and Security)** – All individuals have the right to life, and to live in freedom and safety.
- **Article 5 (Freedom from Inhumane Treatment or Punishment)** – No individuals are to be subjected to torture or to cruel, inhuman, or degrading treatment or punishment.
- **Article 7 (Right to Equal Legal Protection)** – All individuals shall be treated equally in the application of the law and shall be protected by the law without discrimination.
- **Article 9 (Freedom from Arbitrary Detention)** – No individual shall be subjected to arbitrary arrest, detention, or exile.
- **Article 12 (Privacy and Personal Reputation)** – No individuals shall be subject to interference with their privacy or have their reputations impugned.
- **Article 14 (Right to Asylum)** – All individuals have a right to enter a country to seek asylum from the persecution they are experiencing in their home country.
- **Articles 18, 19 & 20 (Freedom of Expression and Belief)** – All individuals have the right to think and believe as they want, including through religious belief and practice. All individuals also have the right to their own opinions, and the right to express them freely.
- **Articles 29 & 30 (Protection of Human Rights)** – The law should guarantee human rights and should allow everyone to enjoy the same mutual respect. Further, no government or non-State entity should act in a way that takes away the rights expressed in the UDHR.

C. The International Convention on the Elimination of All Forms of Racial Discrimination

The International Convention on the Elimination of All Forms of Racial Discrimination ("ICERD") is also particularly relevant to this HRIA.

ICERD is the oldest of the nine core international human rights treaties, and is the principal human rights instrument aimed at eliminating racial discrimination globally.[32] Signatories, including the United States, are bound by international law to protect individuals from discrimination through such efforts as condemning racial discrimination, prohibiting segregation and apartheid, and agreeing to pursue national measures aimed at eradicating racism and promoting racial understanding.[33] In addition to executive policies issued by the President

[32] *See:* "International Convention on the Elimination of All Forms of Racial Discrimination," adopted and opened for signature, ratification and accession by *U.N. General Assembly resolution 2106 (XX)*, December 21, 1965.

[33] *See* Ibid.

and legislation passed by Congress, the United States has a duty to uphold and implement ICERD through public services provisioned by federal and local government agencies.

ICERD elaborates on the non-discrimination articles in the International Bill of Rights, providing a framework expressly dedicated to the elimination of racial discrimination and the promotion of racial inclusion. Companies can draw from ICERD's overarching purpose by bolstering their commitments to the prevention of discrimination against BIPOC communities that may stem from their activities. In addition, they can foster racial inclusion by advancing Diversity, Equity, and Inclusion ("DEI") and racial justice initiatives. Microsoft's efforts toward these goals are addressed below.

D. Applying International Human Rights Framework in this HRIA

Following the UNGPs' expectations for due diligence, and accounting for related international human rights frameworks, the Assessors (1) identify the actual or potential adverse human rights impact(s) with which Microsoft might be involved through its enterprise cloud services and AI technologies, (2) assess whether Microsoft is causing, contributing to, or directly linked to those adverse human rights impacts, and (3) recommend appropriate mitigation strategies in the event of potential harm, and remediation strategies in the event of actual harm.

How to make a determination regarding cause, contribution, or direct linkage is, from the Assessors' perspective, often unclear based solely on the text of the UNGPs inasmuch as the UNGPs do not provide a clear definition regarding corporate relationships to harms or a specific set of evaluative criteria. Further, because the UNGPs are not a source of law, but are instead a set of principles intended to guide businesses in meeting their human rights responsibilities, there is considerable latitude in addressing both the question of causation and the remediation or mitigation strategies that might be available.

Microsoft recognizes the importance of drawing these distinctions. As noted in its most recent Human Rights Annual Report in the context of its 2018 HRIA on AI technology,

> One reason the question of contribution is important is that it can help determine opportunities to use leverage to mitigate potential adverse human rights impacts. Stakeholders pointed to three key factors that could increase the opportunity for leverage: the level of customization, substitutability, and a continuing relationship. These opportunities cannot ensure that adverse impacts won't occur, but they do suggest potential opportunities for companies to exert influence.[34]

The UNGPs call on companies to take positions – even drastic ones that are commercially disadvantageous – to prevent harms by downstream partners for which they could have a level of responsibility. The evaluation of responsibility and attendant action represents a critical due diligence step under the UNGPs. In particular, the Guiding Principles expect that

[34] "2020 Microsoft Human Rights Annual Report," *Microsoft.*

Microsoft will exert its influence to seek the end of serious abuses by the agencies with which the company has a commercial relationship. In instances where this leverage is not significantly effective, the UNGPs call on Microsoft to consider taking positions of greater consequence, namely terminating a particular agency's license or even ending the entire commercial relationship.

In the past, Microsoft has been pressed to end business with certain U.S. government agencies following the revelation of credible evidence indicating systemic human rights abuses by those agencies. Ultimately, Microsoft continued working with the agencies. It is the company's conviction that, in a functioning democratic system with effective rule of law, Microsoft will have greater ability to influence an agency's human rights practices in a positive manner if the two remain in an active commercial relationship. More broadly, by staying in the market, Microsoft would also be able to continue licensing products that adhere to Microsoft's human rights standards—particularly when the use of those products in public services significantly and equitably benefit rights-holders.

As articulated by John Ruggie, the chief drafter of the UNGPs, the connection between harms and a company's responsibilities should be evaluated as a "continuum." Ruggie noted:

> [a] variety of factors can determine where on that continuum a particular instance may sit. They include the extent to which a business enabled, encouraged, or motivated human rights harm by another; the extent to which it could or should have known about such harm; and the quality of any mitigating steps it has taken to address it.[35]

In Ruggie's view, the question of responsibility does not rise or fall on a single factor, but on multiple considerations that are interrelated. Due diligence based on this view should account for a company's enablement, encouragement, and knowledge, in addition to its mitigation efforts.

Similarly, a recent report on corporate responsibility under the UNGPs states:

> The closer the connection between the company's core business operations, specific products, or specific purchasing activities and the resulting harm — balanced with other factors — the greater the likelihood that the company contributed to the harm, and vice versa.[36]

Again, the report notes that the analysis of responsibility rests on multiple factors, including the relationship between the "core" of what a company does and the "specificity" of the activity in relation to the ultimate harm. Professor Vivek Krishnamurthy, reviewing this and

---

[35] "Comments on Thun Group of Banks Discussion Paper on the Implications of U.N. Guiding Principles 13& 17 in a Corporate and Investment Banking Context," *John Ruggie,* 21 Feb. 2017.

[36] Jonathan Drimmer and Peter Nestor, "Seven Questions to Help Determine When a Company should Remedy Human Rights Harms under the UNGPs," *BSR*, January 2021, *available at* https://www.bsr.org/en/reports/seven-questions-to-help-determine-when-a-company-should-remedy-human-rights.

other literature in the context of cloud service provider responsibilities, finds the concept of "specificity" to be analytically significant.[37]

These interpretations help draw a sharper distinction between the cause, contribution, and direct linkage categories through which Microsoft's relationships and responsibilities to harms are determined under the UNGPs. They offer less insight, however, regarding the fine line between direct linkage and relationships in which the contributions of a Microsoft product within a value chain are distant enough from the harm to be immaterial.

In the Assessors' view, when the lines between direct linkage and relationships that fall below such linkage may be blurred, it is advisable for Microsoft to assume it is directly linked and develop a mitigation strategy that diminishes the risk that its products will facilitate harms.

The purpose of the UNGPs is not, like tort law, to find whether there is proximate cause for a specific injury. Determining responsibility for its own sake is not the aim. The purpose of the UNGPs is to "enhanc[e] standards and practices with regard to business and human rights so as to achieve tangible results for affected individuals and communities, and thereby also contribut[e] to a socially sustainable globalization."[38] Accordingly, if responsibility is unclear – as it might often be in a complex digital technology ecosystem – adopting a mitigation strategy will help achieve the UNGPs' objectives in a manner that is consistent with Microsoft's Global Human Rights Statement.

Additionally, although the UNGPs speak in terms of "adverse human rights impacts," the Assessors are mindful that, for a company as complex as Microsoft, actions aimed at mitigating adverse human rights impacts might lead to unintended harms for other rights-holders. For example, Microsoft's enterprise cloud services could be abused by certain actors to serve nefarious ends. Yet it would be disastrous if, in response to this risk, Microsoft stopped selling the cloud services relied on by hospitals, universities, and innovative businesses. In the Assessors' view, and consistent what the Assessors believe to be the spirit of the UNGPs, such binary solutions are neither productive nor necessary. Accordingly, the Assessors consider the full spectrum of human rights implicated in the use of Microsoft's technologies when recommending mitigation strategies, including in the context of law and immigration enforcement.

VI. Microsoft's Human Rights Approach & Policy Commitments

A. Policy Commitments Relating to Human Rights

To gain a broad understanding of Microsoft's human rights commitments and gauge their consistency with internationally recognized frameworks, the Assessors reviewed the policies, guidelines, statements, protocols, and standards that govern the business practices most applicable to this HRIA (collectively, the "Policy Framework").

[37] With Great (Computing) Power Comes Great (Human Rights) Responsibility: Cloud Computing and Human Rights," Vivek Krishnamurthy, *Business and Human Rights Journal*, Edition 7, 2022, page 242.

[38] UNGP, General Principles, Commentary.

Overall, the Policy Framework is robust, intricate, and covers the range of human rights issues related to this Assessment's scope. The documents within the Framework provide significant detail regarding Microsoft's human rights values. The Policy Framework is premised on the principle that "Technology should be used for the good of humanity, to empower and protect everyone and to leave no one behind."[39]

1. Global Human Rights Statement

In the Assessors' view, Microsoft's Global Human Rights Statement is a model to which the human rights programs of other companies in the technology sector can aspire. The Statement articulates the international standards, company initiatives, best practices, and tools that Microsoft applies to evaluate its business activities and fulfill its responsibility to protect human rights.[40]

Critically, the Statement acknowledges that the identity of marginalized groups can intersect with other personal characteristics to increase the already higher risk of harms facing vulnerable rights-holders:

> **Our commitment to vulnerable groups**: Although human rights are universal, they are not yet enjoyed universally. For example, various forms of discrimination require that we pay special attention to vulnerable groups. Vulnerable groups include persons who are disproportionately susceptible to heightened adverse impacts, or those who have less practical access to remedy. We are committed to conducting business without discrimination based on race, color, ethnicity, sex, language, religion, political or other opinion, national or social origin, property, birth or other status such as disability, age, marital and family status, gender, sexual orientation, gender identity or expression, health status, place of residence, economic and social situation, or other characteristics, or the multiple intersecting forms of discrimination that influence the realization of human rights. We commit to take actions to empower vulnerable groups to better exercise their rights.[41]

Microsoft's Statement refers to numerous instruments to which it adheres that address specific types of discrimination, including the International Convention on the Elimination of All Forms of Discrimination Against Women; the Women's Empowerment Principles; the Convention on the Rights of the Child; the Child Rights and Business Principles, the Convention on the Rights of Persons with Disabilities; and the Standards of Conduct for Business on Tackling Discrimination against LGBTI People.[42]

---

[39] *See* "Global Human Rights Statement," *Microsoft.*

[40] Ibid.

[41] Ibid.

[42] Ibid.

The Statement also highlights international initiatives of which Microsoft is a member or supporter, or to which it is a signatory. These initiatives include the Global Network Initiative, the U.N. Sustainable Development Goals, and the U.N. Global Compact.[43]

Pursuant to the Statement, the UNGPs and the OECD Guidelines for Multinational Enterprises serve as the primary frameworks that Microsoft references when designing its human rights due diligence—that is, the primary vehicle through which it assesses, remediates, and mitigates adverse human rights impacts. Microsoft's Statement stresses that it uses "ongoing human rights due diligence" to "understand[] potential human rights impacts associated with digital technologies," which present "unique challenges."[44]

Additionally, the Statement addresses the grievance mechanisms the company provides to stakeholders and rights-holders. These mechanisms are provided through several channels, most notably through anonymous submissions to the company's Integrity Website, complaints emailed to the Business Conduct Email Address, and calls to the Integrity Hotline.[45] Microsoft has also established product-specific channels for voicing grievances, such as the Disability Answer Desk, the Xbox Live Policy & Enforcement, and the Privacy Support Form that allows rights-holders to request the right to access and delete personal data.[46]

The Statement also devotes attention to rule of law and good governance. Specifically, it notes that Microsoft advocates for public policies and laws that promote technological innovation and protect human rights.

Finally, the Statement notes that Microsoft's employees, third-party suppliers and other business partners, and the governments with which Microsoft enjoys a commercial relationship share key responsibilities for implementing the policy. Internally, Microsoft's Regulatory and Public Policy Committee, within its Board of Directors, serves as the primary body for overseeing risks related to the Statement's commitments, and Microsoft's Vice Chair and President is responsible for ensuring that the 1,500 business, legal, and corporate affairs employees sitting within CELA oversee the Statement's implementation.[47]

2. Trust Code

Microsoft's Standards of Business Conduct (which the company refers to as its "Trust Code") seek to maintain and build on the relationships between the company and the stakeholders affected by its operations and activities.[48] The Trust Code states, "Microsoft's Standards of Business Conduct . . . will show you how we will use our culture and values to build and preserve trust with our customers, governments, investors, partners, representatives, and each other, so we can achieve more together."[49] The document categorizes several types of

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid., pages 9-10.

[48] "Trust Code: Standards of Business Conduct," *Microsoft.*

[49] Ibid.

stakeholder relationships, including customers, governments, communities, employees, investors, society, and business partners.[50] The Trust Code seeks to build stakeholder trust by requiring Microsoft's employees and business partners to predicate their decision-making on sound ethical principles that instill confidence in stakeholders affected by Microsoft's activities.

Accordingly, the Trust Code serves as a guidance tool employees can reference when faced with a decision that could compromise the company's values and/or introduce risks. The Trust Code describes several steps employees can take when they have concerns, including an option to ask questions and seek further guidance from CELA and Microsoft's Finance and Human Resources Teams.

The Trust Code also distinguishes between the responsibilities of non-managerial employees and the greater responsibilities of managers and senior executives. Microsoft provides a number of channels to report ethical issues: Microsoft's Integrity Portal; emailing or sending a letter by post to CELA's Office of Legal Compliance; calling a Microsoft hotline; or directly raising concerns with the employee's manager, another Microsoft manager, or the human resources, finance, and CELA Teams. The document also guarantees employees protection from retaliation if they submit allegations of ethical impropriety or human rights violations.

3. Responsible AI Standard

a. Overview

AI is a broad technological concept that encompasses, overlaps with, and sometimes is confused with a variety of other concepts and technologies. AI is notoriously difficult to define—Brad Smith has written that there is "universal vagueness swirling around AI".[51] At the same time, the recent draft of the European Union's proposed AI regulations define AI as "systems that display intelligent behavior by analyzing their environment and taking actions—with some degree of autonomy—to achieve specific goals."[52]

However defined, AI technologies have become increasingly important for the technology industry generally, and Microsoft specifically. Recognizing both the importance of AI and its uncertain effects on human rights, Microsoft helped found the Partnership on AI, which seeks to address ethical issues in the development of AI technologies.[53] It also conducted a human rights impact assessment on AI in 2018. As Microsoft stated in its most recent Human Rights Annual Report, it is difficult to determine responsibility for adverse human rights impacts in the AI context:

> Several factors complicate this question in the context of AI. They include the unpredictability of the nature and use of AI as a rapidly

[50] Ibid.

[51] Smith, Tools and Weapons, 222. *See* also page 224: "There is no universally agreed-upon definition of AI across the tech sector."

[52] "Artificial Intelligence for Europe," *European Commission, April 2018.*

[53] *See* "About Us: Advancing Positive Outcomes for People and Society," *PAI.*

> evolving technology and the complexity of algorithms, which may make it difficult to determine whether the adverse impact stems from the algorithm itself, the data used to train or operate the AI, or the way in which the AI was used. This challenge is more complex for companies that also provide data or cloud computing infrastructure and services enabling customers to build AI products on platforms due to limited visibility into customers' activities.[54]

In light of both AI's potential power and nascency, Microsoft first introduced its Six Principles for AI in 2018.[55] Those principles informed the drafting of Microsoft's Responsible AI Standard (the "Standard"), which it revised in a second version published in June 2022. Microsoft's latest iteration of the Standard significantly augments and formalizes the principles for responsible design and use of AI, and provides extensive guidance and protocols for company personnel engaged in decision-making regarding potentially harmful aspects of AI technologies under development.

The Standard lays out a series of due diligence steps beginning with, and informed by, an impact assessment. Those steps underpin sixteen goals across key areas that Microsoft seeks to achieve when designing and deploying AI technologies. Those goals fall under six categories: accountability, transparency, fairness, reliability/safety, privacy/security, and inclusiveness.

The Standard is supplemented by documentation that provides extensive direction to personnel whose work necessitates due diligence on AI technologies, including the following:[56]

- **The Responsible AI Impact Assessment Template**. The Template allows relevant teams to evaluate a product's likely impacts on rights-holders;

- **The Responsible AI Impact Assessment Guide**. The Guide is a forty-two page resource for teams completing an impact assessment; and

- **Transparency Notes**. Transparency Notes are to communicate to the public the intended uses, capabilities, and limitations of deployed Microsoft AI-dependent products.

The Standard is supported by monitoring tools that assist employees in assessing AI impacts following the deployment of a product, including the HAX Workbook to support early planning and collaboration between engineering disciplines and help drive alignment on product requirements across teams; the AI Fairness Checklist to prioritize fairness when developing AI; and the Fairlearn tool, which seeks to empower AI developers to assess their systems' fairness and mitigate any discriminatory impacts on vulnerable groups.[57]

---

[54] Human Rights Annual Report: Fiscal Year 2021, *Microsoft.* Microsoft's fiscal year 2021 covers the period from July 1, 2020 to June 30, 2021.

[55] *See* "Responsible AI Standard, V2," *Microsoft.*

[56] *See* "Responsible AI Resources," *Microsoft.*

[57] Ibid.

In addition, in 2017, Microsoft established Aether, a body that advises Microsoft's senior leadership on the challenges and opportunities presented by AI technologies. Microsoft has stated that its executives engage Aether to make recommendations on responsible AI issues, technologies, processes, and best practices. The working groups in Aether undertake research and development, and provide advice on rising questions, challenges, and opportunities related to cutting-edge AI.[58]

b. Specific Requirements under the AI Standard

Certain requirements under the Standard establish a formal human rights due diligence process that can help mitigate harms to BIPOC communities emanating from the use of Microsoft's AI products, and design products to prevent future harms from occurring.

At the design stage, for example, the Standard requires Microsoft's AI product teams to carry out due diligence identifying the rights-holders likely to be impacted, stakeholders overseeing the product's use, and those who use the product to make decisions of significant impact on rights-holders. The following requirements provide the parameters for this due diligence:

- "Review defined Restricted Uses to determine whether the system meets the definition of any Restricted Use." (Accountability Goal 1);
- "Identify the stakeholders who are responsible for troubleshooting, managing, operating, overseeing, and controlling the system during and after deployment." (Accountability Goal 5.1);
- "Identify: 1) stakeholders who will use the outputs of the system to make decisions, and 2) stakeholders who are subject to decisions informed by the system." (Transparency Goal 1.1);
- "Identify: 1) stakeholders who make decisions about whether to employ a system for particular tasks, and 2) stakeholders who develop or deploy systems that integrate with this system." (Transparency Goal 2.1);
- "Identify stakeholders who will use or be exposed to the system, in accordance with the Impact Assessment requirements." (Transparency Goal 3.1); and
- "Identify and prioritize demographic groups, including marginalized groups, that may be at risk of experiencing worse quality of service based on intended uses and geographic areas where the system will be deployed. Include: 1) groups defined by a single factor, and 2) groups defined by a combination of factors." (Fairness Goal 1.1).

For each of these requirements, the relevant employees must use the Responsible AI Standard's Impact Assessment Template to document and assess the information collected. To identify and prioritize affected rights-holders, Microsoft recommends communicating with

[58] Responsible AI Webpage, *Microsoft*.

"researchers, subject matter experts, and members of demographic groups," including marginalized and otherwise vulnerable communities.

4. Policies & Initiatives for Addressing Racial Discrimination

Microsoft's products, and the relationships the company cultivates with the agencies that use its products, can themselves mitigate discrimination against BIPOC communities. According to Microsoft's senior managers, the company is committed to implementing DEI principles—including addressing racial injustice as set forth under ICERD—at an enterprise level. This commitment affects the company's operations, activities, and supply chains.

Microsoft recently initiated a number of policy changes that deepen the company's commitments to DEI and racial justice, including committing the company to monitor its progress on the implementation of these goals. As part of this, the company has set goals in the near-term to increase investments in Black-owned businesses, double the number of Black-owned approved suppliers, and spend an incremental $500 million with those entities and existing Black-owned suppliers.[59] Additionally, Microsoft launched the Black Partner Growth Initiative, which focuses on increasing the number of Black-owned business partners in the United States.[60]

Microsoft has initiated numerous efforts related to increased equity and accessibility in the distribution and use of digital technology. For example, it launched the Airband Initiative, to "advance access to high-speed internet and meaningful connectivity" as a "fundamental right."[61] Its TechSpark initiative "[f]oster[s] economic opportunity and job creation in partnership with communities across the U.S."[62] Additionally, its global skills initiative is "aim[ed] at bringing more digital skills to 250 million people worldwide by the end of the [2025]."[63]

Microsoft also created an internal Justice Reform Initiative, which "works to empower communities and drive progress toward a more equitable justice system."[64] As part of this Initiative, the company partners with organizations such as the NYU Policing Project and the National Network for Safe Communities to explore how technology can better advance racial equity in the criminal justice system.[65] Senior executives overseeing Microsoft's racial equity and justice reform efforts emphasized that they work closely with community leaders and civil society organizations to reduce incarceration and advance racial equity in the justice system. These executives indicated that they are empowered by Microsoft both to lobby lawmakers at the state and federal level and to engage directly with civil society organizations through multi-stakeholder coalitions to advance shared racial justice advocacy interests.

---

[59] "Racial Equity: Engaging Our Ecosystem: 2021 Progress Report," *Microsoft.*

[60] Ibid.

[61] "Microsoft Airband Initiative," *Microsoft.*

[62] "The Microsoft TechSpark Program," *Microsoft.*

[63] "Expanding our commitments in Africa: Connectivity and skills" - Microsoft On the Issues *Microsoft*.

[64] "Creating a More Equitable Justice System," *Microsoft.*

[65] Ibid.

Consistent with this HRIA, senior managers responsible for Microsoft's DEI and racial equity policies noted that the company is in the process of internally assessing its civil rights impacts. This process involves evaluating the company's workforce policies and practices and is in progress.

5. Human Rights in Microsoft's Terms of Service

Microsoft's relationships with its customers are governed by their contracts. The applicable documentation varies by product. The Microsoft Azure Product Terms website, for example, provides links to General Service Terms and terms for specific Azure products.[66]

These documents provide contractual and policy restrictions related to Microsoft's products relevant to the impacts addressed in this Assessment. Placing human rights at the center of contractual terms, and ensuring their implementation and enforcement, significantly strengthens human rights due diligence and leads to more effective harm mitigation strategies.

In the Azure General Service Terms, for example, Microsoft restricts use of facial recognition by U.S. law enforcement:

> Customer may not use Azure Facial Recognition Services if Customer is, or is allowing use of such services by or for, a police department in the United States. Violation of any of the restrictions in this section may result in immediate suspension of Customer's use of the service. [67]

As another example, under its Cognitive Services and Applied AI Services, Microsoft references its Code of Conduct for Text-to-Speech integrations. Under that Code of Conduct, the Text-to-Speech implementation by the customer "must not be used to intentionally deceive people" or "disguise policy positions or political ideologies."[68]

Microsoft includes both an "Acceptable Use Policy" and restrictions on "High Risk Use."[69] Under its Acceptable Use Policy, customers may not use products:

- in a way prohibited by law, regulation, governmental order or decree;
- to violate the rights of others; or
- in any application or situation where use of the Services Deliverables could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage, except in accordance with the High Risk Use section below.

In turn, Microsoft's "High Risk Use" terms state:

> WARNING: Modern technologies may be used in new and

---

[66] "Microsoft Azure," *Microsoft.*

[67] Ibid.

[68] "Code of Conduct for Text-to-Speech Integrations," *Microsoft*, July 2022.

[69] "Professional Services," *Microsoft.*

> innovative ways, and Customer must consider whether its specific use of these technologies is safe. The Services Deliverables are not designed or intended to support any use in which a service interruption, defect, error, or other failure of a Services Deliverable could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "High Risk Use"). Accordingly, Customer must design and implement the Services Deliverables such that, in the event of any interruption, defect, error, or other failure of the Services Deliverables, the safety of people, property, and the environment are not reduced below a level that is reasonable, appropriate, and legal, whether in general or for a specific industry. Customer's High Risk Use of the Services Deliverables is at its own risk.

The Assessors did not, however, find any clauses that reference the UNGPs, other international human rights principles and frameworks, or Microsoft human rights policies, nor did they identify any other provisions that would condition the client's use of a Microsoft product specifically on respect for human rights. As noted by one senior executive, Microsoft prefers terms of service that are as all-encompassing as possible, "so they can be uniformly applicable to all sorts of large customers and individual end-users around the world." To this effect, the executive added that contractual clauses usually only indicate that the customer "shall not violate the rights of others."

B. Human Rights Risk Management & Oversight

Microsoft implements its human rights policies in a manner that encourages individual product teams to escalate human rights issues to senior executives and managers in the company's CELA Team. CELA is responsible for driving and overseeing the implementation of Microsoft's human rights policies in its business activities and across its various teams. Consistent with the company's culture and belief that technology, legal, public policy, and human rights issues should not be separately siloed, CELA brings together professionals from across these fields into a single department capable of addressing the full range of such issues and challenges.

Overall, Microsoft's approach to human rights risk management seeks to establish a flexible due diligence process that can be easily and consistently coordinated across relevant teams. All of Microsoft's business groups and product teams are supported by a dedicated CELA Team that provides front-line support on the full range of legal and human rights issues encountered in the development and delivery of products and services. These front-line CELA Teams, in turn, are supported by CELA subject matter experts.

A core responsibility of the front-line CELA Teams is to identify salient legal issues and human rights-related risks – and to escalate these issues to the personnel at CELA who lead Microsoft's human rights efforts, as well as subject matter experts within CELA. All CELA personnel receive training on the identification of risks and the procedures by which to escalate issues to CELA subject matter experts.

The close relationship between the company's business groups and the dedicated CELA front-line team that provides it with legal and human rights support is key to the effectiveness of these processes. Microsoft believes that providing its business groups with dedicated legal, human rights, and public policy professionals residing within CELA assists in the timely and proactive identification of harmful risks as potential products markets, and commercial relationships are considered.

The front-line CELA professionals who support a particular business group are responsible for identifying and mitigating the full range of legal and human rights risks the business encounters and are trained on specific issues relevant to the effective implementation of Microsoft's human rights policies. Front-line CELA personnel have been dealing with human rights issues for years, particularly within Microsoft's cloud businesses aimed at governments and other large customers, and have formed close and productive working relationships with the senior executives in CELA responsible for Microsoft's human rights risk management.

Microsoft describes its human rights management as "hub-and-spoke," intended to empower and support front line personnel to identity and address legal and policy issues, including human rights issues. To that end, Microsoft's teams do not typically follow a formal set of processes and protocols to identify and assess potential human rights risks. As summarized by one senior executive, "Microsoft has a history of being as skinny as it can be, and then relying on qualified personnel in CELA and other teams to identify the human rights challenges that need to be prioritized". This model is intended to create a human-rights-respecting culture, as opposed to one reliant solely on human rights experts.

Consequently, Microsoft has few internal policies and procedures that could be used by personnel as guidance to establish a standardized process for the identification, assessment, and elevation of human rights risks. This makes it particularly important that CELA carry out regular oversight across product teams—especially those working on technologies with features and uses that are at high risk of facilitating serious harms to vulnerable communities.

One executive noted that the small number of CELA team members responsible for Microsoft's human rights implementation and risk management requires them to rely on Front-Line CELA personnel and subject matter experts to make the Team aware of priority human rights issues. The executive indicated that these managers are typically provided with the latitude to act as the "owners and drivers" of their own work portfolios, with CELA standing by to help them manage risks and resolve human rights quandaries when requested. Microsoft finds this approach effective because it places responsibility on front line personnel to be attuned to human rights issues and to escalate them as needed.

Microsoft has a significant record of engaging in human rights due diligence. Since 2016, Microsoft has published an Annual Human Rights Report as a means of providing the public with details on its human rights programs and plans, including the types of due diligence the company conducts, and how it addresses corporate social responsibility ("CSR") expectations

and challenges.[70] Additionally, Microsoft has worked with human rights experts to assess extant and emerging human rights challenges related to its products.

In its most recent Annual Human Rights Report, Microsoft highlighted its 2018 Human Rights Impact Assessment of AI technologies.[71] The Annual Report identified five salient human rights issues as current priorities for human rights implementation, public reporting, and further due diligence monitoring: accessibility, data security and privacy, digital safety, freedom of expression and privacy, and responsible sourcing. As highlighted in this HRIA, these priorities will need to also factor in specific challenges related to racial discrimination in the use of Microsoft's products by high-risk government agencies.

C. Stakeholder Reactions to Microsoft's Human Rights Policies and Practices

Stakeholders primarily commented on Microsoft's Human Rights Statement, DEI work, Responsible AI Standard, and human rights risk management practices.

For each of these policies and practices, stakeholders expressed no complaints or concerns about any specific policy or practice. They did, however, express two holistic concerns. First, that Microsoft's policies are disconnected from its practices. Second, that the company is not transparent regarding its activities. The perceived lack of transparency, in particular, appears to create a negative feedback loop, in which stakeholders view with suspicion whether and to what extent Microsoft has successfully operationalized its commitments.

VII. Salient Adverse Human Rights Impacts

Before considering whether Microsoft bears any responsibility under the UNGPs for human rights harms, it is necessary to first "identify and assess the nature of the actual and potential adverse human rights impacts with which a business enterprise may be involved."[72]

The purpose of this first step is to "understand the specific impacts on specific people, given a specific context of operations."[73] The "specific people" at issue in this HRIA are vulnerable rights-holders, namely BIPOC individuals. The UNGP framework focuses on the most severe harms – based on the scope of harm, scale of harm, and remediability of harm – to which BIPOC are vulnerable.[74]

In the immediate context, Microsoft's products may be connected to the following adverse human rights impacts:

- **Discriminatory surveillance.** This harm involves law enforcement targeting BIPOC communities through surveillance activities and determinations regarding further law enforcement action. Surveillance activities include collecting personal

[70] As a prominent example, *see* "Human Rights Annual Report: Fiscal Year 2021," *Microsoft.*

[71] Ibid.

[72] *See* "Principle 18: Commentary," *UNGPs.*

[73] Ibid.

[74] *See* "Principle 14: Commentary," *UNGPs.*

information (including biometric information), creating databases, and creating predictive policing tools, such as assessments of the risk BIPOC individuals may pose to public safety.

- **Privacy infringement.** Related to discriminatory surveillance, this harm involves disproportionately invading BIPOC communities' expectations of privacy through the collection, storage, and processing of personal data, especially in manners that are not transparent to targeted individuals.

- **Discriminatory arrest and incarceration**. This harm entails collecting, processing, and analyzing information (including that which may be obtained by infringing on the privacy rights of BIPOC individuals) to support high-risk policing activities disproportionately aimed at BIPOC communities. Such harm also increases the likelihood that other fundamental rights will be violated, including the right to life and security, and freedom from inhumane treatment and arbitrary detention.

Each of these harms can be significant in scope and scale. They also connect to, and exacerbate, inequities in the criminal justice system. They are largely ubiquitous, and poorly regulated through state and federal law. To the extent they lead to a loss of life or liberty, they can be impossible for a company to remediate. Notably, these harms may be intertwined with technology products designed to enhance public safety, particularly law enforcement actions that are determined by the collection, storage, processing, and algorithmic assessment of personal data points.

VIII. Assessment of Microsoft's Relationship to Adverse Human Rights Impacts

A. Azure

1. Overview

Azure is a cloud computing platform operated by Microsoft. Both Azure's hardware and software-based operating system form the foundational elements of a digital ecosystem that provides a platform upon which other technology applications can run.

Microsoft licenses hundreds of Azure products, under nearly two dozen categories, including AI and machine learning; analytics; databases; management and governance; and networking.[75] Accordingly, among its options, a customer could have access to Azure Cloud Services, which allows the customer to "build the web and cloud applications you need on your terms while using the many languages we support."[76] Alternatively, the customer could use Azure Automanage, which "offers a unified solution to simplify IT management,"[77] or the

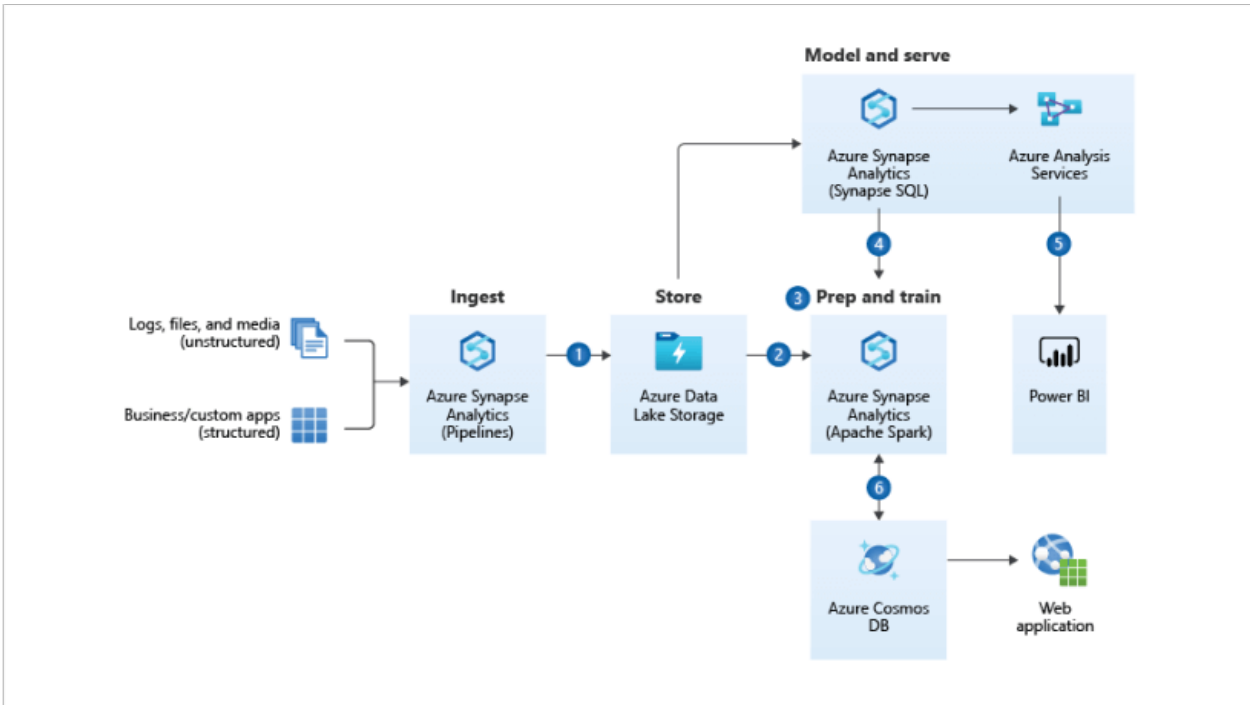
[75] *See* "Azure Products," *Microsoft.*

[76] *See* "Azure Cloud Services," *Microsoft.*

[77] *See* "Azure Automanage," *Microsoft.*

customer could use Azure Traffic Manager, which "operates at the DNS layer to quickly and efficiently direct incoming DNS requests based on the routing method of your choice."[78]

The customer could also combine any number of these Azure products into a package of computing solutions. As an illustration, if a customer were interested in Microsoft's "Cloud scale analytics" solution, it could create a solution architecture using a variety of models that might look like this:[79]



As the above diagram illustrates, this particular architecture solution involves Azure Synapse Analytics, Azure Data Lake Store, Azure Analysis Services, and the Azure Cosmos database. More concretely, under the above architecture, the relevant inputs are received through software applications provided by the customer; are fed to and stored by Azure products that then will use the data to train a machine-learning algorithm; and then will receive specific outputs for various customer purposes.

Regardless of the specific architecture or specific solution, the basic structure of the Azure technology is the same, whether alone or in combination with other Microsoft Azure products and solutions. Namely, Microsoft provides various kinds of tools that can be used by a customer to develop cloud-based solutions specific to that customer. This typically includes running applications developed by the customer on data hosted in the Azure platform. As Microsoft puts it, "[t]he Microsoft Cloud," of which Azure is one part, "provides a unified

[78] *See* "Azure Traffic Manager," *Microsoft.*

[79] *See* "Azure Cloud-Scale Analytics," *Microsoft.*

collection of services for creating applications."[80] Azure is a set of services "aimed at professional software developers who create and maintain new applications."[81]

2. Products marketed for government use

Microsoft specifically markets certain products for government use under its product page "Azure for government."[82] Microsoft's marketing focuses on its products' beneficial uses:

> Deliver services to citizens, anywhere at any time. Modernize your legacy infrastructure and easily scale up and down as needed. Meet government cloud security and compliance standards while managing costs. Learn how governments serve their citizens more effectively with Azure.[83]

Most relevant to this HRIA, Microsoft identifies and promotes certain Azure tools that help governments "enable investigations and analysis":

- **Azure AI**. Azure Applied AI services are a number of services, which are themselves a subset of a suite of AI services that "offer you turnkey AI services for common business processes."[84] Although AI Cognitive Services are "general purpose AI services," Applied AI services have "additional task-specific AI and business logic to optimize for specific use cases." In both cases, they are "designed to help developers create intelligent apps."[85]

- **Azure Media Services.** These services allow licensees to "Manage, transform, and deliver media content with cloud-based workflows."[86]

- **Azure Translator**. Translator allows for the translation of text across 100 different languages.[87]

- **Azure Synapse Analytics**. This service is "a limitless analytics service that brings together data integration, enterprise data warehousing, and big data analytics."[88] There are multiple tools within Synapse Analytics, and for each of

[80] *See* "Build Applications on the Microsoft Cloud," *Microsoft.*

[81] Ibid.

[82] *See* "Azure for Government," *Microsoft.*

[83] Ibid.

[84] *See* "Azure Applied AI Services," *Microsoft.*

[85] Ibid.

[86] *See* "Azure Media Services," *Microsoft*.

[87] *See* "Azure Cognitive Services," *Microsoft*.

[88] *See* "Azure Synapse Analytics," *Microsoft.*

them, developers are provided a workspace upon which they can build customized software solutions. Microsoft provides as examples twenty-four different use cases under four categories: data engineering, data warehousing, data lake, and converged analytics.

These are not the only products that domestic law enforcement licensees may use. The entire suite of Azure products and AI technology is available to government agency customers. Microsoft does, however, tailor its Azure Government services to government licensees, if they choose to use them. The primary difference between what Microsoft calls "Global Azure" and "Azure Government" is in its security features, such as using physically isolated datacenters and networks located solely in the U.S.[89] Otherwise, the Azure products under the "Azure Government" label function similarly to other Azure products: they are platforms on which developers may independently create applications.

Under the category of government solutions, Microsoft specifically markets to "public safety and justice organizations," stating that its products allow those organizations to "make more informed decisions and increase safety for the people and communities you serve."[90] Microsoft regularly blogs[91] and publishes reports detailing various use cases.[92] Some of these publications highlight ways that Azure platforms can help dismantle structural racism and improve public safety.

3. Specific Use Cases

a. Fusion Centers

Fusion centers "are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between state, local, tribal and territorial, federal, and private sector partners."[93] These centers were established to advance national security goals that Congress identified after the September 11th attacks, and were designed to streamline information sharing between federal agencies and state and municipal law enforcement agencies. Key federal agencies involved in fusion centers are the Federal Bureau of Investigation ("FBI"), the Department of Homeland Security ("DHS"), and the Federal Bureau of Prisons ("BOP").

Microsoft provides agencies participating in fusion centers with support for Azure Government and technologies that enable communications interoperability, making it possible for federal and state agencies to exchange intelligence and data between each other and with local police departments.

---

[89] *See* "What is Azure Government," *Microsoft.*

[90] Ibid.

[91] *See* "Microsoft Industry Blogs – Government," *Microsoft.*

[92] For a number of specific cases, *see* "The Future of Public Safety and Justice," *Microsoft,* 2020.

[93] "Fusion Centers," *U.S. Department of Homeland Security,* October 2022.

b. Immigration Enforcement

Two federal agencies bear primary responsibility for immigration enforcement: Immigration and Customs Enforcement ("ICE") and Customs and Border Protection ("CBP"). Both are housed under DHS. These agencies license Azure Government and other Azure tools.[94]

Microsoft has also bid to license its products and services in support of the Repository for Analytics in a Virtualized Environment ("RAVEn"), a new analytical data platform that ICE has been developing since 2018.[95] RAVEn is being designed to analyze large datasets so ICE can more easily identify enforcement targets, as well as patterns and connections between targets and events. RAVEn's databases would purportedly be composed of personal information on public websites, as well as confidential data provided by private sector partners.

Such data could include biometric data from diverse sources, including fingerprints and DNA, official government data, information from social media, surveillance photos and videos, global positioning systems, and financial data obtained from private companies. Notably, RAVEn is identified in the HRIA solely to address potential adverse human rights impacts; RAVEn is not a Microsoft product.

4. Causation Analysis of Azure Products

a. Microsoft's Perspective

Microsoft has two complementary views regarding the use of its technologies by domestic law enforcement and immigration agencies.

The first is that its provision of such technology is done lawfully and with the purpose of providing innovative tools that improve the provision of public safety and national security services to the benefit of all rights-holders, including BIPOC individuals and other vulnerable groups. Although Microsoft recognizes that some of these technologies can be used abusively, from its perspective potential or actual abuse in violation of laws and policies – even if, as a statistical matter, known or reasonably anticipated – does not alone imbue Microsoft with responsibility for adverse human rights impacts. Nor, from Microsoft's perspective, should those adverse impacts outweigh the benefits to public safety and national security when government agencies use such technologies to provision essential public services.

Microsoft's second view is that Azure is a set of cloud computing and AI tools that customers can use (by their in-house IT staff or other third-party IT firms hired by the customer) to develop, deploy, control, and run the customer's own applications and process the customer's own data to serve the customer's purposes. The customer controls its own applications. Customers have the right to protect the confidentiality and privacy of their applications and data from their platform tools providers such as Microsoft. Microsoft agrees that government entities such as law enforcement agencies should be transparent and accountable to the public regarding the applications they develop, deploy, control, and operate and the corresponding impact on the

[94] "Acquisition Planning Forecast System" *U.S. Department of Homeland Security.*

[95] "Amazon, Google, Microsoft, and other Tech Companies Are in a 'Frenzy' to Help ICE Build its Own Data-Mining Tool for Targeting Unauthorized Workers," *Business Insider*, September 1, 2021.

public (including the BIPOC community), and it supports legislative and regulatory reforms toward such public transparency and accountability.

From Microsoft's perspective, consistent with the above descriptions of the products at issue, these services are merely "inert" platforms upon which developers can create and layer software and build out the digital environment they need to perform their functions. The platforms are analytically no different from bridge building materials provided to a city that can be used for both beneficial and abusive means based solely on decisions left to the lawful discretion of the government agency.

In addition, senior executives leading Microsoft's Justice Reform Initiative pointed out that Azure-enabled technology systems can also be harnessed by both police departments and racial justice organizations to provide the data analytics needed to identify racial disparities stemming from public safety practices. That data can then be used to drive more equitable law enforcement practices.

For example, Microsoft partners with Seattle's Law Enforcement Assisted Diversion program, which is designed to provide law enforcement with service delivery in a manner that is aligned with modern restorative justice and decarceration principles. Additionally, the executives noted the company's partnerships with the Vera Institute, the Urban Institute, and the University of Southern California's Sol Price Center for Social Innovation to create virtual tools and multiple data sources that can drive reforms to law enforcement practices and strengthen police engagement with BIPOC communities.[96]

From a more expansive vantage point, Azure Government, and other Azure products, are also being used by local and federal agencies to improve the delivery of social services that are vital to all rights-holders. In the process, agencies have the potential to use Azure to customize their apps in a way that better identifies and corrects situations in which BIPOC and other vulnerable groups may have less access to important services. Azure products, for instance, could be deployed to enable complex data collection and processing that improves the delivery of community and public healthcare programs; police,[97] fire, and paramedic services; humanitarian assistance during natural disasters; and public entitlement programs, such as Medicare, Medicaid, and supplemental food assistance for low-income families.

b. External Stakeholders' Perspectives

Many external stakeholders view Microsoft as the most important technology corporation in the world. In that role, these stakeholders believe that Microsoft has outsized influence over the development and use of a wide array of technologies employed by U.S. agencies. From their perspective, Microsoft's size, importance, and commercial relationships with law and immigration enforcement agencies place special responsibilities on the company. Some of these external stakeholders expressed concern regarding: (1) Microsoft's design of its products; (2) Microsoft's relationships with government agencies, particularly those known to engage in

---

[96] "Empowering Communities Toward a More Equitable Criminal Justice System," *Microsoft on the Issues Blog*, March 2020.

[97] Study: Body-Worn Camera Research Shows Drop In Police Use Of Force : NPR

public safety and national security; and (3) Microsoft's transparency regarding both product design and its commercial relationships with such agencies.

A number of external stakeholders, including those who brought the shareholder resolution, expressed concern that Microsoft has not adequately taken into account how its technologies may enable and reinforce both discrimination and other abuses caused by high-risk government activities – namely, broad data collection, analysis, and surveillance of BIPOC individuals. Accordingly, these stakeholders believe the company should fully assess the potential for its products to amplify these patterns of abuse. More acutely, from the perspective of most civil society representatives interviewed, "but for" Microsoft's development and licensing of these technologies, some of these abuses would not be as effectively facilitated.

These stakeholders expressed particular concern regarding:

- The possibility of flaws in the design of Microsoft products that could reinforce or exacerbate discriminatory targeting of BIPOC and other vulnerable communities by police departments and federal immigration agencies. The stakeholders did not state what these flaws were, but expressed concern that, absent transparency and specific vetting for biases in AI analytical tools, for example, such flaws could exist and enable abusive and discriminatory policing practices;

- The level of support Microsoft may be providing to assist a law enforcement agency's use of a product; and

- The company's failure to incorporate specific human rights expectations into the terms of use and other contractual documents to which government licensees are bound.

Further, many of these stakeholders believe that the use of Microsoft products in policing establishes, at a minimum, a direct linkage between the company and attendant adverse human rights impacts stemming from discriminatory law and immigration enforcement. In some cases, they suggested that Microsoft is not just directly linked, but in fact contributes to harms by law enforcement. From their perspective, contribution occurs when government agencies contract with Microsoft to secure advice regarding potential uses of the agency's Azure platforms—particularly when it is known that the specific law enforcement or immigration agency pursues national security and public safety objectives in a fashion that systematically and disproportionately violates the rights of BIPOC people. ICE stands out as an example of such an agency, although stakeholders also expressed concerns related to an array of local police departments and federal law enforcement agencies.

Finally, stakeholders expressed concern about Microsoft's perceived lack of transparency. The vast majority of civil society representatives, researchers, and socially responsible investment firms conveyed that they do not have a clear window into the suite of Azure products used by local and federal agencies to enhance public safety and immigration enforcement activities. This, they contended, is in large part due to Microsoft not sharing detailed information that would provide a more fulsome picture of its role in strengthening the provision of public services.

c. Government Perspective

The Assessors spoke with three individuals with significant first-hand professional experience in technology and its use by government agencies. These stakeholders had previously served as senior officials in local and federal agencies, with their roles involving the advancement of U.S. national security and public safety objectives, and their impacts on civil liberties. This group was comprised of a former member of a congressionally established federal board, a former attorney and legal advisor at the U.S. Department of Justice, and a former state county prosecutor.

Although their comments on public safety were general, they argued that civil society's criticisms of technology companies' relationships with agencies should be focused on the laws and public policy set by governments, not on the technology providers lawfully developing and providing the technologies. In their view, governments are responsible to citizens, and are legally obligated to protect rights-holders from harms.

The interviewees noted, however, their appreciation of the role technology companies can and should play in strengthening BIPOC communities' enjoyment of rights, arguing that Microsoft's technology can be used to mitigate the harms that end users might cause. They highlighted that AI-based tools could be developed by agencies and built into a cloud computing system to promote socially inclusive national security and public safety objectives. They explained that, although governments should be pressed to establish stronger privacy and non-discrimination protections governing AI's use, technology companies should nevertheless continue to tackle the significant challenges related to racial bias in the design of AI products.

d. Assessors' Analysis

If Microsoft were to be responsible for adverse human rights impacts that emanate from its Azure services as described above, it would, at most, be directly linked to those harms. Under the scenario in which a domestic law enforcement customer is merely licensing products from Microsoft, without more involvement from Microsoft in the development of the products or services, the Assessors do not believe that Microsoft would or could be either causing or contributing to any adverse human rights impacts, as those terms are understood under the UNGPs. If the Assessors were to conclude that Microsoft was directly linked to adverse human rights impacts that emanate from its Azure services, then Microsoft would bear a responsibility to mitigate attendant adverse human rights impacts.

The Assessors believe there are good arguments on both sides regarding direct linkage. On the side in favor of a direct linkage determination, the computing technologies that Microsoft offers—especially when used in combination with each other—are exceptionally powerful, placing in organizations that might not otherwise have the resources, skills, or competence solutions that can be used in myriad ways. Without such technology, advanced surveillance and harms to privacy, in addition to adverse and discriminatory decision-making that comes with AI and analytics technology, would not be possible.

On the side against direct linkage, the Assessors see no evidence that these technologies are anything other than platforms on which end user licensees can develop an array of products

that can be architected into myriad solutions. In this way, cloud platforms and AI technologies are analytically similar to building materials used for any end purpose. The manner in which those materials are provided will inform the level of connection or attenuation between the provider of the materials and the customer, such that the relationship will exist along a continuum. A construction company could provide materials to a customer, which could subsequently build a warehouse or a detention camp. Alternatively, the construction company could build the warehouse itself; whether the warehouse were then used to store medical equipment or illicit drugs would not be in the purview of the construction company. This relationship between platform provider, on the one hand, and developer, on the other, is more or less independent. Wherever the relationship might fall on the spectrum, a "but for" analysis is difficult to justify.

That said, although the "but for" analysis lacks persuasiveness in terms of allocating responsibility, it does suggest that Microsoft should err on the side of mitigation. Government agencies simply do not have the resources to develop products with the kind of sophistication, complexity, and modularity that Microsoft has and can develop. Microsoft's products in fact do enable complex and sophisticated government activity and make easier surveillance and privacy abuses. Moreover, on its website and through social media, Microsoft touts partnerships it has forged with police agencies to end discriminatory disparities in law enforcement and deepen community trust.

Although it is promoting the beneficial role local law enforcement plays in protecting the rights of the communities they serve, Microsoft is simultaneously aware that abuses in policing are systematic, severe, and could be facilitated by technology. Keeping this knowledge at the forefront of Microsoft's human rights due diligence as it develops, licenses, and markets products to law enforcement agencies should be paramount.

This is a challenging fact scenario. Application of the UNGPs does not lead to a clear conclusion that there is direct linkage. Analysis could lead to a conclusion that there is not direct linkage and that, therefore, Microsoft does not bear a responsibility to mitigate any attendant harms. Under the circumstances, and consistent with the spirit of respecting human rights, the Assessors encourage Microsoft to adopt the highest human rights protecting standard and, accordingly, mitigate the actual and potential adverse human rights harms that are connected to the use of its products regardless of the precise degree of its responsibility under the UNGPs. Doing so would not only further Microsoft's own human rights commitments, but also would constitute a best practice.

Notably, as detailed above, Microsoft is already taking extensive steps—and setting industry standards—to mitigate harms through its policies and due diligence process.

Finally, it is important to acknowledge, there is a significant substitutability problem arising out of the question of what Microsoft's appropriate behavior should be in light of its role in the market. The Assessors did not find in discussions with government stakeholders that they would only license solutions from Microsoft. In the absence of Microsoft's product offerings, other parties would fill the vacuum—and those parties may not be mindful of human rights impacts. By staying in the market rather than allowing a competitor to be substituted into a commercial relationship with law enforcement, Microsoft has an opportunity to promote best

practices. This is especially true if Microsoft assumes responsibility to mitigate adverse human rights impacts.

B. Third Party Technologies

1. The connection between third party technologies and Microsoft products

Given the dynamic and modular nature of the suite of Microsoft's products, in particular its Azure cloud products, government licensees have a great deal of freedom to independently develop and/or purchase apps and other technologies that carry out an agency's unique national security and public safety goals.

Microsoft provides access to some of these third party apps through Azure Marketplace.[98] Microsoft describes the Marketplace as "the premier destination for all of your software needs – certified and optimized to run on Azure."[99] Some third party apps are identified as "preferred solutions," which are "selected by a team of Microsoft experts and are published by Microsoft partners with deep, proven expertise and capabilities to address specific customer needs in a category, industry, or industry vertical."[100]

It is important to note, however, that third party apps are developed independently from Microsoft. Even if the third party is a "preferred partner," the third party acts independently from Microsoft in designing, developing, and deploying the app to end users.

Although Microsoft calls certain applications, such as those by Genetec and Veritone below, "preferred solutions," Microsoft executives note that this references technical compatibility, and is not a statement of approval regarding specific end uses.

2. Examples

a. Coptivity

Coptivity is "an AI-enabled conversation mobile app" that "delivers immediate dispatch assistance to deputies on patrol."[101] It is "essentially an intelligent voice assist for law enforcement out on the field."[102] As Microsoft describes one use case for the app in a blog post,

> Instead of calling dispatch to run a license plate or get background information on a driver – and sometimes waiting from 5 to 30 minutes for the results – officers could query Coptivity to instantly identify a vehicle's registration status and the owner's criminal and mental health background.

---

[98] *See* "Azure Marketplace," *Microsoft.*

[99] Ibid.

[100] *See* "Microsoft Preferred Solutions," *Microsoft.*

[101] *See* "Transforming Law Enforcement with the Cloud and AI," *Microsoft*, July 2019.

[102] Ibid.

Microsoft provides additional use case examples in a YouTube video.[103]

The app was created by developers and IT professionals from the San Diego County Sheriff's Department through its participation in Microsoft's HackFest in February 2018. The app uses Azure Government, AI technology, and the Azure Cognitive Services Bot Framework.[104]

b. aiWARE/IDentify

aiWARE is an AI operating system created by the developer Veritone that can be deployed on various cloud platforms, including (but not limited to) Azure Government. Using the aiWARE platform, Veritone created an app in 2018 called IDentify that the company described as a tool for "intelligent, rapid suspect identification."[105] According to the company's description,

> Built upon Veritone's proven AI platform, aiWARE, IDentify empowers law enforcement agencies to substantially increase operational effectiveness by streamlining investigative workflows and identifying suspects faster than ever before. Each day, thousands of law enforcement personnel rely upon the enterprise-scale AI capabilities of aiWARE-based applications to accelerate investigations, protect personally identifiable information, and keep our communities safe.[106]

Veritone primarily markets IDentify to law enforcement agencies. It is offered through Azure Marketplace as a "preferred solution."[107]

c. Genetec

Genetec provides an open-platform software, hardware, and cloud-based service designed to help law enforcement agencies streamline and strengthen their public safety response. This service – the "Genetec Security Center" platform – is offered on Azure Marketplace as a "preferred solution." The Security Center is a "unified platform that blends IP video surveillance, access control, automatic license plate recognition, intrusion detection, and communications" in a single solution.[108] Video surveillance includes intelligent cloud-based, closed-circuit television ("CCTV"), and other forms of video-based activity monitoring. Genetec's surveillance software has been licensed to law enforcement departments in U.S. cities, such as Atlanta.[109]

---

[103] *See* "Improving Situational Awareness in Law Enforcement with Microsoft AI," *Microsoft.*

[104] Transforming Law Enforcement with the Cloud and AI," *Microsoft*, July 2019.

[105] *See* "Applications: Identify," *Veritone*.

[106] Ibid.

[107] https://azuremarketplace.microsoft.com/en-us/marketplace/apps/veritoneinc.veritone_identify?tab=Overview

[108] *See* https://azuremarketplace.microsoft.com/en-us/marketplace/apps/genetec.securitycenter?tab=overview

[109] "How Securing Atlanta for the Big Game Became an Access Management Initiative," Case Study, *Assa Abbloy*.

d. Offender 360

Offender 360 was developed in 2014 by Tribridge, a technology services firm specializing in business applications and cloud solutions.[110] In designing Offender 360, Tribridge used the cloud-based Microsoft Dynamics Customer Relations Management ("CRM") software that is hosted on Azure Government.[111]

Offender 360 brings together previously siloed information databases to create a holistic view of an incarcerated individual. Individuals are then compared against others in the database and categorized on this basis. Offender 360 is intended to create precise data profiles that identify individuals most likely to benefit from court diversion programs, education, skills, and job preparedness programs offered in prisons, and coordination of a person's reentry into society.[112] In addition, it is designed to monitor and manage prison populations, and reduce violence, recidivism, and other risks to the safety of both incarcerated individuals and corrections officers.

The State of Illinois purchased licenses for the use of the CRM platform and made use of Microsoft's technical support agreements to train their correctional staff on how to customize applications.[113] It has since been adopted and further developed by other correctional facilities across the country.[114]

3. Causation Analysis of Third Party Apps

a. Microsoft's Perspective

From Microsoft's perspective, third party apps are developed by government customers and third-party companies that serve the public sector independently of Microsoft. Microsoft does not believe it has a direct linkage to such app developers that triggers responsibility for downstream harms within the digital ecosystem that uses its products. Microsoft has noted that it is an upstream platform developer and that its products can be used for countless applications created by the licensees. Moreover, Microsoft believes that the above cases show how third parties are developing public safety tools to uphold the freedoms and human rights, including the right to safety, of all rights-holders. Microsoft notes that government agencies use Azure products to develop and integrate apps that improve an array of social services and other public initiatives. These technologies have immense potential to protect and advance human rights and well-being if they are developed and used in a manner that prevents bias.

---

[110] "Microsoft Power BI – U.S. Partners," *Microsoft.*

[111] "Day 28: Big Leap in Inmate Tracking: Offender360 Accelerating Illinois' Modernization – a 30-day blog," *Illinois Department of Innovation and Technology*, March 2016.

[112] *See:* "How AI Can Empower Correctional Facilities and Their Clients," *Microsoft Industry Blogs – Government*, August 2019.

[113] "CRM Lands in Jail: Meet Illinois Offender 360," *Information Week*, February 2013.

[114] "Offender 360: Solution Overview," *DXC Technology*, 2020.

b. External Stakeholders' Perspectives

Although civil liberties and racial justice organizations did not have visibility into any relationships or partnerships between these apps and Microsoft, they did express nearly universal concern about the nature of Microsoft's involvement in their development and design.

Animating the concerns from civil society stakeholders were specific abuses that could be possible with these third party apps. For example, because Coptivity was designed by a police department, and allows for rapid and real-time voice-assisted database searching regarding sensitive information about individuals, stakeholders expressed concern about the capability of Coptivity to exacerbate discriminatory and abusive policing. Likewise, they observed that Veritone's IDentify could be used as an abusive surveillance tool. Additionally, Genetec's CCTV-based products increase the scope of BIPOC rights-holders who may be harmed by racially discriminatory policing practices.

Genetec's products used by the Atlanta police department raised particular concerns among these stakeholders. According to one group, the Atlanta Police Department has over 10,000 CCTVs equipped with the technology. The presence of so many security cameras raises concerns that cities such as Atlanta are using the technology to conduct mass surveillance that can make it easier for police to target suspect activities in Black-majority neighborhoods.

On the other hand, some researchers, human rights organizations, and socially responsible investment firms highlighted the ways Azure products are used, or could be used, to develop beneficial apps. Examples include apps that can help identify BIPOC and other underserved communities when determining how critical-need services should be delivered.

Nevertheless, from the perspective of these civil society groups, Microsoft is likely to be at least directly linked to the adverse human rights impacts stemming from these technologies. Some civil society groups also believe that if Microsoft plays a role in the design and development of the apps, then it may be contributing to such harms.

c. Government Perspective

The individuals representing the government perspective reiterated that the abusive use of technology is not the primary fault of the technology developer, and that civil society advocacy should be focused on the laws, policies, and regulations that govern law enforcement practices and the use of technology by law enforcement. To the extent these technologies can facilitate discriminatory abuses, and because the current legal authorities for regulating the technology sector are outdated, they argued that Microsoft should take care to develop technologies and set expectations for their use that can reduce the risk of harms.

d. Assessors' Analysis

Similar to their view regarding the licensing of Azure products to government licensees, the Assessors do not believe it necessary to assign a formal level of responsibility when Microsoft is simply providing a platform on which developers create third party apps that may be used in beneficial or abusive ways. As a best practice, to address the possibility of harms

occurring downstream, Microsoft should mitigate the actual and potential adverse human rights harms that are connected to the use of its products regardless of whether it has a formal responsibility to do so under a UNGPs analysis.

The significant steps that Microsoft is already taking during the regular course of business to mitigate harms through its policies and due diligence set a leadership position within the industry, and can be expanded to account for possible harms by the third party entities involved in Microsoft's value chain.

C. Law Enforcement Digital Systems

1. New York Domain Awareness System

In 2012, in an effort to combat terrorism, the New York City Police Department (NYPD) "coordinated with Microsoft to develop a networked Domain Awareness System (DAS)."[115] Although "originally designed as a counterterrorism platform," the DAS is currently "a program that aggregates a substantial quantity of the information NYPD personnel use to make strategic and tactical decisions."[116] NYPD describes DAS as providing the capability to:

- Efficiently access critical information such as real-time 911 information, past history of call locations, crime complaint reports, arrest reports, summonses, NYPD arrest and warrant history, as well as a person's possible associated vehicles, addresses, phone numbers, date of birth, and firearm licensure history;
- Distribute wanted posters and missing person alerts among NYPD personnel;
- Share photos of arrests and the physical description of someone arrested by NYPD; and
- Issue critical alerts on any matters or potential threats at queried locations.[117]

To operationalize these capabilities, DAS takes advantage of CCTV cameras in each of the five boroughs. NYPD personnel can use DAS to view live feed from the cameras. DAS further acts as a central database to access information obtained by license plate readers, although DAS software itself does not read license plates.[118] DAS also uses "ShotSpotter," a gunfire/gunshot detection system.[119]

According to Microsoft, NYPD and the company "jointly developed DAS by bringing together Microsoft's technical expertise and technologies with the day-to-day experience and

---

[115] "NYPD Domain Awareness System: Impact and Use Policy," *NYPD*, April 2021; Also *see* "New York City Police Department and Microsoft Partner to Bring Real-Time Crime Prevention and Counterterrorism Technology Solution to Global Law Enforcement Agencies," *Microsoft.*

[116] Ibid.

[117] Ibid.

[118] Ibid.

[119] Ibid.

knowledge of NYPD officers."[120] Microsoft called the ensuing solution "tailor made to meet the specific needs of its users." The agreement between NYPD and Microsoft allowed NYPD to receive "30 percent of revenue from the sales of the DAS system to other customers worldwide."[121] When Microsoft developed the system it intended to more broadly carry "the solution to market in an effort to extend these capabilities to other jurisdictions," noting that "[p]ublic safety organizations interested in deploying DAS will go through a process of customization based on [the] unique" requirements of the law enforcement agency.[122]

2. Other Law Enforcement Digital Systems

Microsoft also develops other technologies that law enforcement can use built on Azure, sometimes referred to as "Microsoft Aware" or "Microsoft Aware Solution," maintained by Microsoft Consulting Services.[123] Some information suggests that Aware can be tailored by an individual police department to its own data needs.[124] Generally speaking, Aware can be used with geospatial data, detailed maps, photography and descriptions of critical infrastructure and neighborhoods, and integrate real-time footage from video cameras placed around a city, including CCTVs mounted on a pole, cameras on a police vehicle's dashboard, and cameras worn by police officers.[125]

According to Microsoft, Aware is not a policing solution or SKU that the company replicates and duplicates, because different agencies have different needs. Rather, at its core, Aware provides law enforcement officers a single pane of glass dashboard to view relevant law enforcement information, replacing the need to having a law enforcement officer log into multiple databases to retrieve existing data points. Aware takes the place of such field work by looking into separate systems and using API calls to other solutions to retrieve information from those other solutions. The Aware solution is not limited to police departments: the same single pane of glass dashboard concept can be used by other industries. At the time of this HRIA's publication, the Assessors did not find any references to Aware Solution systems on Microsoft's website.

Microsoft executives noted that Aware "does not contain any editing features, and does not have the ability to change the accessible information." Further, it "does not use video analytics or any biometric measurement technologies." Although Aware "does not use facial recognition technologies and cannot conduct facial recognition analysis," still images within Aware "may be used as a probe image for facial recognition analysis."[126]

---

[120] "New York City Police Department and Microsoft Partner to Bring Real-Time Crime Prevention and Counterterrorism Technology Solution to Global Law Enforcement Agencies," *Microsoft.*, https://news.microsoft.com/2012/08/08/new-york-city-police-department-and-microsoft-partner-to-bring-real-time-crime-prevention-and-counterterrorism-technology-solution-to-global-law-enforcement-agencies/

[121] Ibid.

[122] Ibid.

[123] "Microsoft Aware Solution, *Microsoft.*

[124] "Microsoft Aware Solution: Datasheet," *Microsoft Consulting Services*; "Overview of Microsoft Aware Solution," *Microsoft*;

[125] "Microsoft Aware Can Help Police Departments around the World Operate Effectively," *MSpowersuser.com*.

[126] Ibid.

According to a 2016 Microsoft blog,

> Over the last several years, Microsoft has partnered with several progressive law enforcement agencies around the world to develop a set of capabilities known as Microsoft Aware.
>
> Aware uses Microsoft's modern Azure capabilities including big data and business intelligence platforms to help first responders develop a common operating picture based on aggregated data from multiple sources. By connecting to gunshot sensors, for example, Aware can not only alert police officers when a gun has been fired, but also correlate that alert with additional information such as license plate readers (LPRs), 911 call information, warrant and arrest data. The resulting capability allows officers and their command staff to understand the context of the alert with much greater detail. By connecting that information with real-time footage from video cameras placed around the city–whether they are mounted on a pole, in a vehicle's dashboard, or body-worn on an officer—Aware can automatically rewind the video cameras closest to the alert so police officials can quickly see what is happening in the area before, during, and after the shot was fired.
>
> Aware can be connected to geospatial data to show the exact location of nearby critical infrastructure and facilities such as schools and subway stations. This allows officers to immediately understand if there are additional considerations needed when responding to a call for service. Aware also supports maps, photography and descriptions of critical infrastructure to allow an officer to navigate unfamiliar territory.[127]

Other police departments appear to have adopted Microsoft systems similar to DAS, including the Washington D.C. Metropolitan Police Department (D.C. MPD).[128] The system was operational in 2014, but Microsoft has not provided any enhancements, customizations, or ongoing maintenance support to the D.C. MPD since April 2016, and the system is no longer in use.

3. Causation Analysis of DAS and Other Law Enforcement Digital Systems.

[127] "Improving Situational Awareness for Police Officers", Industry Blogs, *Microsoft,* June 2016.

[128] "Inside D.C.'s Sprawling Network of Surveillance," *The Intercept*, https://theintercept.com/2022/06/18/dc-police-surveillance-network-protests/ .

a. Microsoft's Perspective

Microsoft underscores that DAS does not run on Azure. For clarity, Microsoft referred the Assessors to the NYPD's guidance on DAS, which notes that use of data made available through DAS is subject to the NYPD Domain Awareness System Impact and Use Policy, which states:

> DISPARATE IMPACTS OF THE IMPACT & USE POLICY The safeguards and audit protocols built into this impact and use policy for DAS mitigate the risk of impartial and biased law enforcement. DAS is a program that centralizes a large quantity of lawfully obtained data, information and resources to aid NYPD personnel in making tactical and strategic decisions. DAS does not use video analytics, facial recognition, or any other biometric measurement technologies.
>
> The NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights. The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution, Sections 11 and 12 of Article I of the New York State Constitution, Section 14-151 of the New York City Administrative Code, and other applicable laws.
>
> Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action. When an officer's decision to initiate enforcement action against a person is motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not just race, age, and gender, but other identifying characteristics or information.[129]

Microsoft strongly supports use of policies such as these whenever police engage the public, whether in connection with use of digital technologies or otherwise. Microsoft notes that the benefits of digital systems developed and used appropriately by law enforcement agencies ("law enforcement digital systems") include lives saved, the protection of people and their property, and the opportunity to more effectively collect and use data that helps law enforcement identify and correct racial disparities in policing. Microsoft's efforts in this regard are addressed in Section VI(A)(4).

b. External Stakeholders' Perspectives

Nearly all the racial justice and civil liberties organizations with which the Assessors spoke expressed significant concerns about Microsoft's involvement in the creation and

[129] *See* https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/domain-awareness-system-das-nypd-impact-and-use-policy_4.9.21_final.pdf

promulgation of the NYPD's DAS system. From their perspective, Microsoft did not merely license generic products to these customers, but instead tailored specific products that Microsoft was aware could, and likely would, be used in an abusive manner. Moreover, many of these stakeholders believe that Microsoft used its partnership with NYPD to refine the generic architecture of other law enforcement digital systems in order to sell such products to police departments across the U.S. and in other countries.

Civil liberties groups and racial justice advocates highlighted the ability of law enforcement digital systems—whether DAS or others—to collect and process myriad sensitive data points that describe individuals' physical features, criminal records, and mental health records. These stakeholders noted that the technologies can be used to disproportionally monitor BIPOC communities for perceived threats to public safety.[130] They added that any human rights harms resulting from these applications are almost certain to affect these communities in an equally disproportionate manner. In their view, Microsoft's technologies could amplify the deep-rooted tendency by law enforcement to perceive BIPOC—in particular Black men—as criminal threats.

The racial justice and civil liberties groups believe that law enforcement digital systems are overly focused on the aspects of public safety that relate to perceived security threats. They noted that the algorithmic risk assessment tools that police departments may integrate into these surveillance systems are likely to preserve racial biases that are structurally embedded in American society. This tendency, they added, should be mitigated by inserting human oversight in key phases of the algorithmic decision-making process.

One privacy rights organization also questioned whether Microsoft knows what biometric and other personal data sources are being integrated into DAS and other law enforcement digital systems, and the extent to which the technical support provided by Microsoft may be helping "make the information usable by law enforcement" when determining what response is needed, to whom it should apply, and in what neighborhoods.

Broadly speaking, most organizations believed that DAS specifically is an example of various law enforcement tools that Microsoft helps develop and deploy with little to no input from human rights organizations. None of the stakeholder groups interviewed indicated that they were asked for input when the products were developed and sold to the NYPD. If the products are still being developed and sold or licensed, they are not being made aware of this. These groups emphasized that their input could include possible safeguards to prevent potential misuse or ensure the app does not generate emergency dispatch responses that discriminate against BIPOC individuals.

Some organizations discussed reporting on the use of Azure platforms and Microsoft surveillance technologies by Israeli law enforcement. Although an international example, the

[130] "The Anti-Blackness of Surveillance," Dario McCarty, *Berkeley Political Review,* January 20, 2021; "The Disparate Impact of Surveillance," Barton Gellman and Sam Adler-Bell, *The Century Foundation,* December 21, 2017; "Race, Surveillance, Resistance," Arnett, Chaz, *Ohio State Law Journal*, Vol. 81, No. 6, 2020, pp. 1103-1142; "There is Overwhelming Evidence That the Criminal Justice System is Racist. Here is the Proof," *The Washington Post*, June 10, 2020.

organizations argued that Microsoft is effectively "test piloting" its surveillance technologies abroad in order to refine law enforcement digital systems licensed to U.S. law enforcement.

c. Government Perspective

The former government officials who spoke with the Assessors argued that law enforcement digital systems hold the potential to help produce positive public safety outcomes. By working with police departments, technology companies such as Microsoft can better create useful public safety tools and help mitigate potential abuses through the development of those tools. They also contend that to the extent these technologies can lead to abusive uses, in the absence of regulation Microsoft can and should seek to use its technology to mitigate such harms.

d. Assessors' Analysis

From the Assessors' perspective, there is a substantial difference between creating generic products that can be licensed to third parties and aiding in the creation of specific products. DAS provides a prominent and detailed example of Microsoft's assistance in creating systems used by law enforcement. Aware—provided through Microsoft's consulting services—appears to present similar opportunities as DAS does to help Microsoft tailor products for law enforcement agencies. This is notwithstanding that Aware is not a dedicated law enforcement product.

Although the creation and licensing of a platform that can be used for myriad purposes can be "linked" to a downstream adverse human rights impact, the UNGPs are not concerned with "mere" linkage. They are concerned with "direct" linkage. Providing a platform in the stream of commerce is akin to providing parts to build a bridge or a car, or paper to write a book. Such materials may be used for nefarious ends, but that is not their purpose, and the upstream business entity cannot be held responsible for all downstream abuses.

The matter is different, however, if the business participates in the development of specific uses intended by the downstream customer. Under the UNGPs, the question of direct linkage is tied to the company's "own activities" or "as a result of [its] business relationships with other parties."[131] John Ruggie's interpretation of the UNGPs' allocation of responsibility, quoted above, is helpful in describing factors that can identify how close or attenuated the connection is between the company and the downstream harm, including "the extent to which a business, enabled, encouraged, or motivated" the human rights harm, or "could or should have known about such harm."[132] Additionally, as the Drimmer and Nestor report put it, "[t]he closer the connection between the company's…specific products…the greater the likelihood that the company contributed to the harm."[133]

---

[131] "Commentary on Principle 13," *UNGPs*.

[132] "Comments on Thun Group of Banks Discussion Paper on the Implications of UN Guiding Principles 13& 17 in a Corporate and Investment Banking Context," *John Ruggie*, February 2017.

[133] "Seven Questions to Help Determine When a Company should Remedy Human Rights Harms under the UNGPs," *BSR*, January 2021.

The Assessors do not believe Microsoft causes or contributes to harm through the creation and deployment of law enforcement digital systems. Although the UNGPs do not provide a clear test for contribution, the UNGP interpretive guide provides examples that may be illuminating. Contribution could occur, for example, where an enterprise is "[p]erforming construction and maintenance on a detention camp where inmates were allegedly subject to inhumane treatment." Direct linkage, in contrast, might occur where a business "[p]rovid[es] financial loans to an enterprise for business activities that, in breach of agreed standards, result in the evictions of communities."[134]

The development of a cloud platform with attendant AI technologies, customized to a solution for law enforcement and aimed to enhance public safety, does not fit neatly with either example, but seems closer to the provision of a loan intended for a legitimate purpose than the construction of a detention center for a nefarious one. Certainly, the creation of law enforcement digital systems is not, in Ruggie's words, "encouraging" or "motivating" downstream harms. To the extent that (a) systems are specifically developed in partnership with police departments, and (b) systemic privacy, surveillance, and discriminatory policing abuses by police departments are enabled by such technologies, then the Assessors believe Microsoft would be directly linked to the adverse human rights impact stemming from the law enforcement digital systems.

The question of contribution is not an academic one. If the Assessors were to conclude that Microsoft contributes to adverse human rights impacts relating to the creation of law enforcement digital systems, the company would have a responsibility under the UNGPs to remediate actual harms; it has no such responsibility if it is directly linked. Although the Assessors do not believe that Microsoft is contributing under the UNGPs to adverse human rights impacts relating to DAS, the question is a close one. Accordingly, Microsoft may wish to consider taking and/or supporting remediating activities as a way of demonstrating leadership when responsibility is unclear.

The Assessors recognize policing abuse is not the purpose of law enforcement digital systems. The Assessors also recognize the important public safety function such technologies play, and the work that Microsoft does to mitigate harms and use its technology to prevent the harms that may stem from it. As the UNGPs stipulate, "Business enterprises should not undermine States' abilities to meet their own human rights obligations." Surely, ensuring public safety is a human rights obligation, and Microsoft does well to provide government agencies the tools to meet those obligations.

The benefits produced by such technologies, however, do not "offset" the adverse human rights impacts that may ensue through their use.[135] In concluding that there is a direct linkage in this situation, the Assessors also underscore Microsoft's responsibility under the UNGPs to mitigate against harms that arise from policing technologies that are more bespoke in nature than generic products.

Mitigation in response to direct linkage does not mean that Microsoft should necessarily cease providing consultation to police departments. Indeed, such consultation creates an

[134] "Interpretive Guidance to Principles 17," *UNGPs*. interpretive guide, 17, *available at*

[135] Ibid.

opportunity for Microsoft to identify challenges that can lead to human rights harms and work with government agencies to mitigate both potential flaws in the technologies and the misuse of those technologies.

IX. Recommendations

To guide Microsoft as it continues to develop cutting-edge products to help government agencies enforce the rule of law and protect the human rights of citizens writ large, the Assessors offer a series of recommendations. The recommendations reflect the Assessors' best judgement – based on their expertise at the nexus of business and human rights – regarding actions that could most effectively help Microsoft mitigate against the possibility that its products could be directly linked to salient harms to BIPOC and vulnerable communities by government agencies.

The recommendations also respond to Guiding Principle 24 of the UNGPs, which notes "[w]here it is necessary to prioritize actions to address actual and potential adverse human rights impacts, business enterprises should first seek to prevent and mitigate those that are most severe or where delayed response would make them irremediable."[136] To this end, the recommendations are ordered from highest to lowest priority within each issue category.

Issue	Recommendation
	1. To strengthen and clarify its commitment to respect for human rights, and non-discrimination in particular, Microsoft should consider updating its Global Human Rights Statement by: (A) Clarifying that employees are expected to implement commitments in the Statement that apply to their work responsibilities; and (B) Noting that Microsoft encourages its customers to act in a manner that is consistent with Microsoft's human rights commitments, as well as the rule of law regarding respect for human rights, when using its products and to mitigate any adverse impacts on rights-holders. 2. To strengthen the Responsible AI Standard's commitments to human rights, and non-discrimination in particular, Microsoft should consider:

[136] The commentary on Guiding Principle 34 further explains "While business enterprises should address all their adverse human rights impacts, it may not always be possible to address them simultaneously. In the absence of specific legal guidance, if prioritization is necessary business enterprises should begin with those human rights impacts that would be most severe, recognizing that a delayed response may affect remediability. Severity is not an absolute concept in this context but is relative to the other human rights the business enterprise has identified".

Issue	Recommendation
Policy Framework	(A) Adding case studies for assessing the use of AI-based products by law enforcement agencies in the Responsible AI Standard's Impact Assessment Guide; and (B) Soliciting direct feedback from rights-holders, civil society representatives, community leaders, government agencies deploying AI-based products, and lawmakers who oversee those agencies regarding the deployment of such products on BIPOC and other vulnerable stakeholders. 3. Microsoft should consider adding a set of human rights-related options to the Trust Code's Integrity Portal form that employees submit when screening ethical issues and other concerns. This could include additional prompts focused on vulnerable groups, including when an employee believes the design, development, and/or use of a Microsoft product could lead to a violation of Microsoft's commitments to the rights of vulnerable groups. Microsoft might also consider providing a link in its Trust Code to relevant grievance mechanisms in the Global Human Rights Statement.
Policy Oversight & Risk Management	4. As a best practice, Microsoft might consider taking and/or supporting activities to remediate actual harms when it has provided consulting services to help develop cloud and AI products for domestic law and immigration enforcement agencies and responsibility is unclear. Such remediation could include technological innovations, additional resources, and funding for racial justice-based initiatives in communities where such harms are prevalent. Microsoft could explore opportunities to conduct the remediation in partnership with law enforcement licensees, relevant judicial and correctional systems, civil society organizations, and/or affected communities. 5. Implementing Microsoft's human rights commitments and objectives across the company's many applicable teams is a significant challenge. Microsoft should consider how, within its existing structure or a different structure, the CELA Team responsible for human rights implementation can strengthen its ability to conduct and oversee human rights risk management across the company's relevant teams.

Issue	Recommendation
Policy Oversight & Risk Management	6. To ensure continuity with respect to external engagement, the CELA Team could manage the new stakeholder engagement strategy that is described in the Stakeholder Engagement recommendations below. 7. To help ensure broader consistency with the company's human rights policies and mitigate against possible harms, the CELA Team and Office of Responsible AI should consider conducting oversight of third-party app developers and Microsoft's commercial partners that are part of a government licensee's digital value chain. 8. The CELA Team and the Office of Responsible AI should consider what tools Microsoft can use to prohibit novel AI technologies that create the highest risk of facilitating serious discriminatory harm, such as synthetic and generative AI, from being used in a harmful manner, without prohibiting their beneficial uses, such as helping to empower vulnerable groups and making public services more accessible and efficient. 9. Microsoft should consider developing and maintaining a database within CELA that includes information regarding: (A) The due diligence assessments the company has conducted on high-risk products, including those used by government agencies; and (B) The beneficial and adverse impacts from the use of those products on BIPOC and other vulnerable communities.
	10. In the Terms of Use and other clauses in its contracts with government agencies, Microsoft should consider referencing its Global Human Rights Statement as an expression of its commitments to human rights and encouraging the government agency to respect the rights of stakeholders pursuant to its obligations under the law. 11. Where appropriate and legally permissible, Microsoft should consider supporting an agency's implementation of remediative steps by offering to provide human rights-based training.

Issue	Recommendation
Relationships with Federal Government & Local Law Enforcement Agencies	12. Where appropriate and legally permissible, Microsoft should also consider carrying out such training to an agency engaged in high-risk activities *before* providing a product. 13. Per the UNGPs guidance on the application of leverage, Microsoft should encourage government licensees and other partners in Microsoft's digital value chain to uphold the company's human rights commitments – in particular, non-discrimination – in their respective activities. 14. If Microsoft is presented with credible information indicating that a government licensee is using its products in a way that violates Microsoft's commitment to non-discrimination and/or other human rights commitments, and Microsoft remains committed to conducting business with that agency, then the company should consider taking additional steps to mitigate against such human rights harms, including by: (A) Engaging in consultation and training with appropriate agency personnel; and (B) Engaging in consultation with human rights experts, including representatives of civil society, regarding best practices in addressing such challenges and in promoting accountability. 15. To improve implementation of the Responsible AI Standard, for use cases that present the greatest risk of serious discriminatory harm, Microsoft should consider revisiting the due diligence that was conducted according to the Standard's requirements when the use case was being reviewed to ensure the Standard is being followed and to identify any due diligence gaps.
	16. Microsoft should consider developing a strategy to ensure the company is engaging with key stakeholders who advocate on the human rights issues addressed in this HRIA. Such a strategy could be co-developed and implemented by the CELA Team responsible for Microsoft's human rights implementation and the Office of Responsible AI. 17. To help make the strategy effective, Microsoft should consider conducting a stakeholder mapping exercise with the objective

Issue	Recommendation
Stakeholder Engagement	of capturing a broad set of perspectives from civil society and other stakeholders. 18. Microsoft should consider establishing a dedicated communications channel that civil society organizations and other stakeholders can use to provide comments and share information regarding the human rights impacts of Microsoft's products. Such an initiative could include a response protocol that prioritizes concerns based on severity of the harms to vulnerable rights-holders. 19. Microsoft should consider ways to collaborate with civil society and other organizations to develop shared principles, goals, and actionable steps regarding advocacy for legislative and regulatory reforms to the commercial technology sector. 20. Microsoft should consider expanding its partnerships with research centers, racial justice advocates, and police departments to increase the positive impacts of data-driven justice initiatives supported by Microsoft products.
Human Rights Due Diligence **Human Rights Due Diligence**	21. Microsoft should consider opportunities to engage with civil society, rights-holders, human rights experts, community leaders, and representatives of law enforcement organizations to discuss the findings and recommendations in this HRIA and potential priorities for future human rights due diligence. Microsoft should prioritize those groups that participated in this HRIA. 22. Microsoft should consider conducting theme-specific due diligence exercises or additional HRIAs focused on: assessing the company's effectiveness in implementing the remediative and mitigating steps proposed in this HRIA's recommendations; assessing the company's commercial relationships with military agencies and their impacts on BIPOC and other vulnerable communities; and other human rights challenges prioritized by the stakeholder organizations with which it engages. 23. Microsoft should consider using this HRIA as a reference in its ongoing internal civil rights assessment, particularly with respect to that assessment's evaluation of racially

Issue	Recommendation
	discriminatory impacts of Microsoft products on rights-holders.

ANNEX A

Organizations Interviewed that Agreed to the Publication of Their Names

Name of Organization	***Number of Individuals Interviewed from Organization***
Access Now	1
Action Center on Race and the Economy (ACRE)	1
American Friends Service Committee (AFSC)	1
Boston Common Asset Management	1
Brennan Center for Justice at the NYU School of Law	1
Color of Change	1
Culper Partners LLC	1
Domini Impact Investments	1
Electronic Frontier Foundation (EFF)	1
Empower LLC	1
Heartland Initiative	1
Human Rights Watch	5
Information Society Project at Yale Law School	1
Interfaith Center for Corporate Responsibility (ICCR)	2
Investor Advocates for Social Justice (IASJ)	1
Jewish Voice for Peace (JVP)	2
Open MIC	1
Secure Justice	1
Snohomish County Prosecuting Attorney's Office	1
Total	25