At Microsoft, respecting human rights is a critical component of our mission to empower every person and every organization on the planet to achieve more. Focus on human rights helps our employees to make good decisions and ethical choices, and builds trust with our customers and partners.

The Microsoft Global Human Rights Statement explains our commitment to respecting and promoting human rights >
Highlights

Microsoft Technology & Human Rights Center – We continued our human rights due diligence on artificial intelligence, and continued to implement our 5-year partnership between Microsoft and the UN’s Office of the High Commissioner for Human Rights as well as partnerships with other organizations.

Artificial intelligence – We launched the free AI Business School online, announced our facial recognition principles, and launched our AI for Humanitarian Action program.

Accessibility – New accessibility products were launched including the Adaptive Controller for Xbox, new accessibility updates to Windows 10, Skype and the Seeing AI app, and our Inclusive Hiring program has resulted in over 100 individuals with disabilities including autism being hired in Microsoft.

Data security and privacy – Since General Data Protection Regulation (GDPR) went into effect over 18 million people around the world have used Microsoft’s Privacy Dashboard to control their personal data and exercise GDPR privacy rights, which Microsoft has extended to all of our consumer customers worldwide.

Freedom of expression and privacy – Microsoft successfully completed the third independent assessment of our implementation of the Global Network Initiative (GNI) principles.

Online safety – We became a signatory to the Christchurch Call to Action, the Global Internet Forum to Counter Terrorism (GIFCT) made progress in its mission to disrupt terrorists’ ability to use the internet in furthering their causes while also respecting human rights, and the continued to grow our Digital Civility Index.
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Microsoft Technology and Human Rights Center</td>
<td>6</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>13</td>
</tr>
<tr>
<td>Accessibility</td>
<td>24</td>
</tr>
<tr>
<td>Data security and privacy</td>
<td>30</td>
</tr>
<tr>
<td>Freedom of expression and privacy</td>
<td>39</td>
</tr>
<tr>
<td>Online safety</td>
<td>43</td>
</tr>
<tr>
<td>Sustainable Development Goals</td>
<td>50</td>
</tr>
<tr>
<td>Glossary of abbreviations and technical terms</td>
<td>53</td>
</tr>
</tbody>
</table>
Introduction

Annual human rights reports are a key element of our commitment to transparently communicate Microsoft’s ongoing efforts to respect human rights. As defined in the UN Guiding Principles on Business and Human Rights (UNGPs), we continue to implement a variety of policies and processes across a range of salient human rights risks to avoid infringing on the human rights of others and to address adverse impacts with which we are involved.

The primary focus of this report is on our efforts to respect human rights, but it also touches on Microsoft’s efforts to promote and advance human rights. The report is perhaps most useful for rightsholders and stakeholders who are specifically interested in our systematic work to implement the UNGPs. However, we invite all readers to use this resource to help us advance our implementation and performance.

This report covers the Fiscal Year 2019 (FY19; July 1st, 2018 to June 30th, 2019), and is made available on the human rights page of the Microsoft Global Corporate Social Responsibility (CSR) reporting website. Please visit the CSR reporting website for more information on Microsoft’s policies and practices related to human rights, as well as policies and practices related to other economic, environmental, and social issues.
Microsoft Technology and Human Rights Center

Established in 2013, the Center prioritizes and coordinates our human rights due diligence, identifies emerging risks and opportunities related to human rights, and promotes harmonized approaches to human rights across the company. The Center also fosters dialogue to advance understanding of the human rights impacts of information and communication technology (ICT). Through the Center, Microsoft engages with a broad range of human rights groups, academics, and industry groups globally to share Microsoft’s experiences and lessons learned.

The Center is not alone in its efforts to ensure Microsoft respects human rights. It is complimented by numerous teams across the business who are responsible for the day-to-day management of our human rights risks.
Microsoft’s [Global Human Rights Statement](#) outlines our commitment and approach to respecting the rights of our employees, product users, suppliers and individuals in the communities in which we operate. This statement applies to Microsoft and all its subsidiaries. This approach is aligned with the UNGPs, which is the authoritative global standard for business and human rights, and our membership in the [Global Network Initiative](#) (GNI), which is a collaborative approach to protect and promote freedom of expression and privacy in the ICT sector.

The Statement was last updated in FY17. We aim to ensure that our policy commitment evolves in line with the ever-changing global human rights environment and to ensure that the Statement reflects the lessons we continuously learn through our growing human rights experience. The Statement is available in 12 languages and was approved by Microsoft’s President and Chief Legal Officer.

The Statement includes:

- Explicit recognition that technology is increasingly an essential gateway to the exercise of human rights
- Special consideration to vulnerable groups such as children, women and people with disabilities
- Champions the rule of law informed by consideration of international norms

The latest updates to the Statement were surfaced through consultations in organized workshops and bilateral interviews with technical and policy experts across the globe to understand their experience of Microsoft’s human rights work, and to uncover opportunities for continual improvement. Workshops and meetings were held with academic, civil society organizations, and practitioner experts in the fields of business, ICT, and human rights across North America, Europe and Asia to ensure that Microsoft’s approach reflects a broad range of stakeholder expectations.

That initiative also served to identify a singular aspiration for the Microsoft Technology and Human Rights Center:

Microsoft aspires to leadership in business and human rights and to serve as a catalyst for action by others – in the technology sector and beyond.
The Microsoft Technology and Human Rights Center has adopted a four-part strategy to pursue this aspiration:

**Class-leading due diligence** – We aim to conduct best-in-class human rights impact assessments on salient Microsoft action and emerging trends in business and human rights.

**Rights-aware decision making** – We are deploying an integrated approach to human rights decision making across key aspects of Microsoft.

**Proactive engagement** – We use actions and public statements to demonstrate that Microsoft is an important voice and advocate for the promotion of human rights.

**Transparent leadership** – We are advancing transparency in our work to respect and promote human rights through increased disclosure and engagement.

We use these categories to frame the Center’s activities in our annual human rights reports.

**Class-leading due diligence and rights aware decision making**

As discussed in our previous annual human rights reports, we began a major forward looking Human Rights Impact Assessment (HRIA) at the start of FY17 into Microsoft’s growing portfolio and expertise in artificial intelligence (AI). The first round of that HRIA was completed in FY18, and more information was provided in the dedicated AI section of the FY18 human rights report.

A key finding from the FY18 HRIA on AI was the need to better understand an important expectation of the UNGPs in the context of the AI value chain; determining when a company may be causing, contributing or is directly linked to adverse human rights impacts related to its business activities and what that means for a business’ responsibility to address human rights impacts. Throughout FY19 we undertook an exercise to assess this issue and that is outlined in more detail in the dedicated AI section of this report.
Proactive engagement

In January 2019, Microsoft’s Executive and Senior Leadership hosted its annual human rights roundtable at the World Economic Forum’s Annual Meeting in Davos. This year’s roundtable focused on how technology companies, governments and civil society can apply human rights principles to build trust in AI technologies. The meeting was co-hosted with our longstanding partners at New York University’s Stern Center for Business and Human Rights.

In order for AI to benefit everyone, AI’s design and deployment must avoid harms to human rights, and human rights frameworks can help to foresee some of AI’s potential social impacts and to create policy and technical safeguards to stimulate positive uses. However, human rights are not yet at the center of prominent AI debates. Without respecting the universal and binding norms embodied in the global human rights regime, we face the risk of a commercial race to the bottom.

Technology and human rights experts from academia, civil society, government, industry and international organizations explored questions including:

- Key barriers and solutions to integrating human rights practices into company structures and processes, such as engineering, design, policy, and legal.
- Human rights issues arising from the use of facial recognition, including bias, privacy and freedom of assembly and association.
- How governments, civil society and technology companies can collaborate on regulation, shared principles and transparency.

The panelists for the discussion were the UN High Commissioner for Human Rights, Michelle Bachelet, the Director of the Center for Business and Human Rights at New York University’s Stern School of Business, Michael Posner, and Microsoft’s President and Chief Legal Officer, Brad Smith. Nicholas Thompson, Editor in Chief of Wired Magazine, acted as moderator.

Microsoft’s membership of the World Economic Forum is an important vehicle for cross-company and cross-industry human rights collaboration to help inform and advance our human rights priorities, and Microsoft continues to serve as a member of the Global Future Council on Human Rights and the Fourth Industrial Revolution where
we support the Council’s work on frontier technologies and implications for human rights.

In FY18 we co-hosted a half-day conference in June 2018 in Brussels titled Protecting Democracy in a Changing World alongside the UN’s Office of the High Commissioner for Human Rights (OHCHR), and the NYU Stern’s Center for Business and Human Rights. Media, human rights, and technology experts from academia, civil society, EU institutions, government and industry explored questions including how to rebuild trust in media, technology, governments and democratic processes; how human rights is being influenced by democracy and technology; and how governments, media and technology can collaborate on cybersecurity, misinformation, and civic engagement.

As part of the UN’s UDHR 70 campaign, the meeting in Brussels was held to mark the 70 years since the Universal Declaration of Human Rights (UDHR) was proclaimed by the UN General Assembly. The purpose of the campaign was to engage a broad base of audiences the world over to help promote understanding of how the Universal Declaration empowers us all, and to encourage further reflection on the ways that each of us can stand up for rights, every day.

In FY19 we also celebrated UDHR 70 in New York and in Singapore. In October 2018, Microsoft, in partnership with Business for Social Responsibility (BSR), hosted a workshop on Artificial Intelligence, Business, and Human Rights: Addressing the Intersection. The half-day workshop featured an overview of BSR’s research on AI and the UN Guiding Principles on Business and Human Rights as well as insights from Microsoft on our HRIA of AI.

Interactive futures sessions were used to explore innovative approaches to anticipating issues and how to take tangible steps toward implementing the UNGPs in a future-proof manner. The target audience for the workshop was non-tech companies who might currently see AI as being an issue on the horizon, or even over the horizon, but who were keen to begin their human rights due diligence in advance. That supports Microsoft’s intention of helping customers navigate their digital transformation responsibly. Roundtable discussions included:

- The human rights issues arising from the use of AI in the financial services, retail, healthcare, and transportation industries.
Key barriers and solutions to integrating human rights practices into company structure and processes, such as engineering, design, policy, and legal.

Finally, a Human Rights Impact Assessment Masterclass was held in Singapore in December 2018 with a view to provide as practical a learning opportunity as possible. The full day workshop was delivered in partnership with BSR, the Business and Human Rights Resource Center, and the UN Development Program’s (UNDP) business and human rights program in the Asia-Pacific.

The interactive workshop focused on how Asian companies can understand and apply the UNGPs in practice, using real-world case studies and practical exercises to explore the realities of conducting and implementing actionable HRIAs. In-house counsels, CSR practitioners, government affairs professionals, government officials and civil society representatives explored questions including:

- The human rights impacts arising from business activities across Asia, including in low-, middle- and high-income countries, and across sectors including manufacturing, natural resources and services.
- The barriers and solutions to integrating HRIA findings and recommendations into company processes and risk management, such as operations, business development, policy, and legal affairs.

In FY17 we reported on a new academic partnership with the University of California, Berkeley’s Human Rights & Business Initiative which is a joint initiative of UC Berkeley’s Haas School of Business and the Human Rights Center. Through an annual technology, business and human rights conference, student consulting projects, and other collaborative efforts, UC Berkeley and Microsoft are aiming to integrate key human rights issues such as privacy, inclusion, freedom of expression, education and employment directly into business education.

Our first joint conference in FY17 was on the topic of Big Data and Artificial Intelligence: The Human Rights Dimension for Business. In FY18 our conference was on the topic of the Future of Work. The FY19 conference was on AI for Social Impact.

Co-sponsored by the Human Rights Center of Berkeley Law, the Center for Responsible Business at Haas School of Business, and the Microsoft Technology and Human Rights Center, the goal of the 2019 conference was to build greater awareness of the positive
impact of AI, but also recognize the potential downsides, risks, or unintended consequences of this technology while building solutions intended to have positive social impact. This third annual conference explored the role and responsibility of businesses to scale AI for social impact, ranging from large-scale global challenges, such as poverty, education, and disease, to local issues that disproportionately affect vulnerable groups.

The conference brought together students, practitioners, and experts from business, academia, and civil society to discuss:

- How business can develop, use, and scale AI to address local and global challenges
- How business can scale AI in a responsible way that does not infringe on human rights
- How business can collaborate with key stakeholders to maximize the positive impact of AI

**Transparent leadership**

Statistical reporting comprises an important component of our transparency. On a biannual basis Microsoft publishes [Content Removal Requests Reports](https://www.microsoft.com/en-us/privacy/requests-policy), [Law Enforcement Requests Reports](https://www.microsoft.com/en-us/privacypolicy/requests-policy) and the [U.S. National Security Orders Reports](https://www.microsoft.com/en-us/privacy/requests-policy). Each report provides detailed Q&A on topics including what precisely is covered in each report, the processes we administer when adjudicating how to respond to the related requests for content moderation and user data, and, importantly, the rights of rightsholders in relation to the three reports. We hope that the reports can be a useful tool for rightsholders to determine how they can best exercise their rights online.
Artificial intelligence

At Microsoft, we think of AI as a set of technologies that augment human capabilities. AI enables computers to perceive, learn, reason and assist in decision-making to solve problems in ways that are similar to what people do. Key technologies include:

- **Vision** – The ability of computers to “see” by recognizing what is in a picture or video.

- **Speech** – The ability of computers to “listen” by understanding the words that people say and to transcribe them into text.

- **Language** – The ability of computers to “comprehend” the meaning of the words.

- **Knowledge** – The ability of a computer to “reason” by understanding the relationship between people, things, places, events and the like.

Beginning in the previous human rights report, we continue to include a section dedicated to AI and human rights in recognition of the important on-going work in the ICT industry, civil society and governments to advance responsible AI.

**Principles**

Our responsibilities in developing and deploying AI have been maturing for some time now. In June 2016, Microsoft’s CEO, Satya Nadella, published *Principles for Responsible AI*. The principles stated that the “most critical next step in our pursuit of AI is to agree on an ethical and empathic framework for its design”.

We expanded upon those principles in October 2016 when we released our free online book, *The Cloud for Global Good*. The book lays out Microsoft’s policy roadmap to ensure that cloud technology is trusted, responsible and inclusive. The roadmap includes 78 policy recommendations across 15 areas including privacy, security, environmental sustainability, artificial intelligence, public and cybersecurity, human rights, education and jobs skills training. The Cloud for Global Good articulates
Microsoft’s view of the steps which governments, the technology industry, and civil society can take to build cloud technology that serves the broader good.

In FY18 we went further by also publishing our book *The Future Computed: Artificial Intelligence and its role in society*. Released in January 2018, *The Future Computed* explains our perspective on the future of AI; principles, policies and laws for the responsible use of AI; and AI and the future of jobs and work.

Principles are critical to addressing the societal impacts of AI and building trust as the technology becomes more and more a part of the products and services that people use at work and at home every day. The six principles that we believe should guide the development of AI are:

- **Fairness** – When AI systems make decisions about medical treatment or employment, for example, they should make the same recommendations for everyone with similar symptoms or qualifications. To ensure fairness, we must understand how bias can affect AI systems.
- **Reliability** – AI systems must be designed to operate within clear parameters and undergo rigorous testing to ensure that they respond safely to unanticipated situations and do not evolve in ways that are inconsistent with original expectations. People should play a critical role in making decisions about how and when AI systems are deployed.
- **Privacy and security** – Like other cloud technologies, AI systems must comply with privacy laws that regulate data collection, use and storage, and ensure that personal information is used in accordance with privacy standards and protected from theft.
- **Inclusiveness** – AI solutions must address a broad range of human needs and experiences through inclusive design practices that anticipate potential barriers in products or environments that can unintentionally exclude people.
- **Transparency** – As AI increasingly impacts people’s lives, we must provide contextual information about how AI systems operate so that people understand how decisions are made and can more easily identify potential bias, errors and unintended outcomes.
- **Accountability** – People who design and deploy AI systems must be accountable for how their systems operate. Accountability norms for AI should draw on the experience and practices of other areas, such as healthcare and
privacy, and be observed both during system design and in an ongoing manner as systems operate in the world.

**Actions**

To help ensure that these six principles are integrated into our development and deployment of AI, the Microsoft AI and Ethics in Engineering and Research (AETHER) Committee was formed in FY18. This committee is an internal organization that includes senior leaders from across Microsoft’s engineering, research, consulting and legal organizations. It focuses on proactive formulation of internal policies and on how to respond to specific issues as they arise.

The AETHER Committee considers and defines engineering best practices, provides guiding principles to be used in the development and deployment of Microsoft’s AI products and solutions, and helps resolve questions related to ethical and societal implications stemming from Microsoft’s AI research, product and customer engagement activities.

Externally, Microsoft joined with Amazon, Facebook, Google and IBM in September 2016 to co-found the Partnership on AI (PAI). Its membership has been expanded to include academic experts and civil society. The remit of PAI is to conduct research, organize discussions, share insights, provide thought leadership, consult with relevant third parties, respond to questions from the public and media, and create educational material that advances the understanding of AI technologies including machine perception, learning, and automated reasoning.

We are also a founding sponsor of the Business Roundtable on Human Rights and AI which is being convened by Article One. The Roundtable seeks to promote the development of responsible AI using human rights as its underlying framework, through a mixture of peer learning, by supporting the member companies of the PAI, and with direct engagement of AI and human rights experts.

We recognize that the AI and ethics debate must include a dedicated application of human rights norms and principles by not just Microsoft, but also by the many other actors who are integral to developing and deploying AI applications. International human rights laws and norms helps to build technologies with safeguards that respect the rights of individuals and help avoid or minimize adverse impacts on individuals and communities, especially vulnerable groups.
To help business leaders navigate questions of how and where to implement AI; the cultural changes that AI requires companies to make; and how to build and use AI in ways that are responsible, protect privacy and security, and comply with government rules and regulations, we launched an **AI Business School** in FY19.

The free online course is a master class series that aims to empower business leaders to understand challenges and opportunities in the age of AI. Course materials include case studies and guides, videos of lectures, perspectives and talks. Short introductory videos provide an overview of the AI technologies driving change across industries, but most of the content focuses on managing the impact of AI on company strategy, culture and responsibility.

The business school complements other AI learning initiatives across Microsoft, including the developer-focused **AI School**, which provides job-ready skills and real-world experience to engineers and others looking to improve their skills in AI and data science. Content focused on responsible AI allows users to earn about the implications of AI in both business and government. Materials include guidelines to setting up principles and a governance models in organizations, as well as resources, best practices, and tools.

Turning to facial recognition, we know that the technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression. That’s why, in the US, we have called for a government initiative to regulate the proper use of facial recognition technology, informed by a bipartisan and expert commission.

We believe there are three problems that governments need to address:

- Especially in its current state of development, certain uses of facial recognition technology increase the risk of decisions and, more generally, outcomes that are biased and, in some cases, in violation of laws prohibiting discrimination.
- The widespread use of this technology can lead to new intrusions into people’s privacy.
- The use of facial recognition technology by a government for mass surveillance can encroach on democratic freedoms.
That call for action does not absolve companies like Microsoft from taking actions. In addition to this call for action we are continuing our efforts to reduce bias in facial recognition. The improvements are intended to address serious concerns that commercially available facial recognition technologies more accurately recognize the gender of people with lighter skin tones than darker skin tones, and that they performed best on males with lighter skin and worst on females with darker skin.

Additionally, based in part on input from the AETHER Committee, we are moving more deliberately with our facial recognition consulting and contracting work. This has led us to turn down some customer requests for deployments of this service where we have concluded that there are greater human rights risks.

We are also aiming to be an active voice in the facial recognition debate. We have established a transparent set of principles for facial recognition technology. In part this will build on our broader commitment to design our products and operate our services consistent with the UNGPs.

In December 2018 we introduced the principles that will guide Microsoft in how we develop and deploy facial recognition technology. The principles are:

- **Fairness** – We will work to develop and deploy facial recognition technology in a manner that strives to treat all people fairly.
- **Transparency** – We will document and clearly communicate the capabilities and limitations of facial recognition technology.
- **Accountability** – We will encourage and help our customers to deploy facial recognition technology in a manner that ensures an appropriate level of human control for uses that may affect people in consequential ways.
- **Non-discrimination** – We will prohibit in our terms of service the use of facial recognition technology to engage in unlawful discrimination.
- **Notice and consent** – We will encourage private sector customers to provide notice and secure consent for the deployment of facial recognition technology.
- **Lawful surveillance** – We will advocate for safeguards for people’s democratic freedoms in law enforcement surveillance scenarios and will not deploy facial recognition technology in scenarios that will put these freedoms at risk.

Learn more about these principles >
To help implement the principles, we released a Transparency Note in FY19 for developers to understand how the Azure Face API (Face API) works, the choices that can be made by system owners that influence accuracy, and the importance of thinking about the whole system, including the technology, the people, and the environment. Available through Azure Cloud Services, Face API detects, recognizes, and analyzes human faces in images using pre-trained machine learning models that have been developed by Microsoft. Developers can integrate Face API functions into their systems without creating their own model.

The Transparency Note covers topics including understanding accuracy and errors, best practices for improving accuracy, and deploying responsible facial recognition systems.

**Human rights due diligence**

While our FY18 Al HRIA served to clarify potential human rights impacts and opportunities to mitigate those impacts, it also surfaced new questions. A key finding from our FY18 HRIA was the need to better understand an important expectation of the UNGPs in the context of the AI value chain; determining when a company may be causing, contributing or is directly linked to adverse human rights impacts related to its business activities and what that means for a business’ responsibility to address those human rights impacts. To understand the distinction between contribution and directly linked to, Microsoft partnered with Article One to review relevant literature and survey leading experts on this topic.

According to the UNGPs a company’s responsibility to respect human rights includes a responsibility to:

- “Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;”
- “Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.”

Determining when a company causes an adverse human rights impact can be relatively clear, while understanding the distinction between when a company is “contributing” to
rather than being “directly linked” to an adverse impact can be less clear. Understanding the grey areas between either contribute and directly linked, however, is even less clear and remains difficult in the context of AI.

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

Stakeholder engagement resulted in a recommendation to align factors for contribution across sectors. In addition, a recommendation emerged to assess the degree to which the unique nature of both the deployment and development of AI can provide opportunities for leverage as part of the human rights due diligence process.

Given this, guidance from OHCHR to the banking sector was used to assess the degree to which that guidance could inform similar questions when it came to AI.

- **Contribute**: “A bank can contribute to an adverse impact through its own activities (actions or omissions)\(^1\)—either directly alongside other entities, or through some outside entity, such as a client. Contribution implies an element of ‘causality’, for example that the bank’s actions and decisions influenced the client in such a way as to make the adverse human rights impact more likely. This element of causality may in practice exclude activities that have only a ‘trivial or minor’ effect on the client, which may thus not be considered as ‘contribution’.” For example: “A bank provides financing to a client for an infrastructure project that entails clear risks of forced displacements may be considered to have facilitated—and thus contributed to—any displacements that occur, if the bank knew or should have known that risks of displacement were present, yet it took no steps to seek to get its client to prevent or mitigate them”

- **Linked**: “Direct linkage’ refers to situations where a bank has not caused or contributed to an adverse human rights impact, but there is nevertheless a direct

---

\(^1\) OHCHR defines a bank’s "own activities" as “actions and decisions (including omissions) involving third parties, such as providing financial products and services to clients.”
link between the operations, products or services of the bank and an adverse human rights impact, through the bank's business relationships.” For example: “A bank may be one of several financiers to a project where a client, in breach of agreed standards and the client’s own policies, violates health and safety regulations in a way that puts workers’ health at risk. In this case, the bank has not contributed to the adverse impact. However, once it is made aware of this situation, it should use any leverage it has over the client to seek to mitigate the impact”.

However, stakeholders pointed to a number of important considerations when it came to leverage. Indeed, 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.

**AI for Good**

Through our AI for Good platform we aim to use the benefits of AI to empower others in new and more impactful ways to help create a more sustainable future, by providing seed grants of technology to organizations, and capacity building tools and resources.

At the start of FY18, we announced the launch of our AI for Earth program. AI for Earth puts Microsoft’s cloud and AI tools in the hands of those working to solve global environmental challenges. Through grants that provide access to cloud and AI tools, opportunities for education and training on AI, and investments in innovative, scalable solutions, AI for Earth works to advance environmental and ecological sustainability across the globe.

Towards the end of FY18, we also announced the launch of our AI for Accessibility program. This program harnesses the power of AI to amplify human capability for the more than one billion people around the world with a disability, since AI can empower people with disabilities with tools that support independence and productivity, as technology rapidly changes the way we live, learn, and work.
In September 2018 we announced a third AI for Good program; **AI for Humanitarian Action**. Our aim is to expedite new AI solutions as quickly and broadly as possible in four areas:

- **Disaster response** – Artificial intelligence and data modeling hold huge promise for forecasting and detecting early signs of coming disasters, and also can help responders better target their aid. AI technologies like machine vision can quickly analyze images of roads damaged or destroyed by an event, making way for a faster and safer response. In a new partnership with the World Bank, United Nations and partners from the tech industry, relief organizations will be better able to predict when and where future famines will occur so aid can arrive earlier, potentially saving more lives.

- **Needs of children** – We believe AI can equip NGOs and organizations with better tools to protect the world’s most vulnerable population: children. Human trafficking, for instance, is one of the world largest criminal industries, ensnaring millions of children each year. Already we are using predictive analytics and bot frameworks to target both the supply and demand underpinning human trafficking – ultimately disrupting criminals and bringing relief to victims around the world.

- **Refugees and displaced people** – AI and machine learning have the potential to improve the lives of the approximately 68 million displaced people in the world, 28 million of whom are refugees. AI can help optimize the delivery of aid, supplies and services to refugees and can scale NGOs’ efforts to communicate and understand displaced peoples’ needs. Microsoft is already working with the Norwegian Refugee Council, NetHope and University College Dublin to develop a chatbot using AI technologies, such as language understanding, machine translation and speech recognition to intelligently assist displaced youth to connect them with free, high-quality educational resources.

- **Human rights** – We will collaborate with NGOs and humanitarian organizations to accelerate breakthrough solutions to help monitor, detect and prevent human rights abuses. Deep learning has created the ability to better predict, analyze and respond to critical human rights situations. Utilizing AI-powered speech translation, people can connect with pro bono lawyers who are protecting people’s human rights.

Discover all of Microsoft’s AI for Good programs >
**TrialWatch**, a major program to stem from the AI for Humanitarian Action program, was launched in April 2019. The program trains and equips trial monitors to document and determine whether trials are conducted in a fair way. This is a partnership between the American Bar Association, the Clooney Foundation for Justice, Columbia Law School, Microsoft and OHCHR.

AI-powered text to speech and language-translation capabilities speed the input of data and enables experts around the world to help assess a trial’s fairness even if they don’t speak a local language. With this information, and backed by data science capabilities, the Clooney Foundation can build quantitative and qualitative reports that will be reviewed and evaluated by its legal experts.

Learn more about where TrialWatch is being deployed >
**Salient human rights issues**

The [UN Guiding Principles Reporting Framework](http://www.un.org/guidingprinciples) recommends that companies focus their human rights reporting on their *salient human rights issues*, which are the “human rights at risk of the most severe negative impact through the company’s activities and business relationships.”

Saliency focuses on the risk to people, not the business, whilst also recognizing that there is a strong convergence between the risks to human rights with risk to the business.

While a business can touch upon a broad spectrum of human rights, the Reporting Framework identifies that the most salient human rights issues consist of four factors:

- **Most severe** – Based on how grave and how widespread the impact would be and how hard it would be to put right the resulting harm.
- **Potential** – Meaning those impacts that have some likelihood of occurring in the future, recognizing that these are often, though not limited to, those impacts that have occurred in the past.
- **Negative** – Placing the focus on the avoidance of harm to human rights rather than unrelated initiatives to support or promote human rights.
- **Impacts on human rights** – Placing the focus on risk to people, rather than on risk to the business.

The following sections of the report apply the UN Guiding Principles Reporting Framework to Microsoft’s current salient human rights issues.
**Accessibility**

With respect to Article 9 of the Convention on the Rights of Persons with Disabilities, which states that persons with disabilities have the right to access, on an equal basis with others, to information and communications technologies to live independently and participate fully in all aspects of life, we create and deliver technology that is accessible and functional for people of all abilities.

**Approach**

Our Chief Accessibility Officer leads Microsoft’s Accessibility team. The team is responsible for establishing and leading the implementation of our accessibility policies and practices across our business, including in engineering, human resources and marketing.

In support of the Accessibility team’s work, a cross-company advisory team, led by our Chief Accessibility Officer, consists of technical leaders and accessibility champions within key engineering groups. This advisory team is accountable for delivering accessibility commitments across Microsoft by auditing the status of projects and by prioritizing workstreams in product roadmaps.

We employ three guiding principles in our approach to accessibility:

- **Transparency** – We are open with our plans to ensure our products are accessible.

- **Accountability** – We prioritize inclusive design and accessibility in the upstream development process of all products and services.

- **Inclusivity** – We want everyone to be empowered – not only through our products, services and technology, but also within our culture at Microsoft.

Each product group is responsible for delivering on our corporate commitment to develop accessible products.
Working with governments and civil society organizations is a core component of our approach to delivering technology benefits to people with disabilities. For example, Microsoft is a signatory of the Charter of the Global Initiative for Inclusive Information and Communications Technology (G3ict). The Charter encourages governments to increase digital inclusion of citizens by incorporating accessibility criteria into public procurement.

Our commitment to accessibility is publicly shared at microsoft.com/accessibility.

**Policies**

Recognized accessibility standards guide product development and testing for business operations across Microsoft, including:

- The European Standard on accessibility requirements for Information and Communication Technologies (ICT) products and services (EN 301 549)
- Section 508 of the US Rehabilitation Act (29 U.S.C. 794d)
- The Web Content Accessibility Guidelines (WCAG) 2.1, ISO/IEC 40500

Internal guidance and training are regularly updated in light of evolving industry standards, regulations, and market needs. Proactive communication with NGOs, customers, and policymakers helps us inform and, where possible, validate our roadmaps.

We strive to provide rightsholders with opportunities for direct engagement and support. In the context of accessibility, we recognize our responsibility to help users resolve any queries they have related to Windows and Office, and with third-party assistive technologies. Support is provided to consumers through the Consumer Disability Answers Desk (DAD) and to enterprise customers through the Enterprise Disability Answer Desk (eDAD).

Both answer desks resolve the queries in real time or with engineering teams to identify potential future fixes. The support team is trained in using many popular assistive technologies and can help in English, French, and Spanish through phone or online chat, and American Sign Language (ASL) via videophone in the US with agents who have a hearing disability and are fluent in ASL.

DAD: Click here to connect with the Consumer Disability Answers Desk >
In FY17 we reported that the average number of customer contacts received by the DAD per month was 20,000, which was double the average number of contacts per month in FY16. That increase coincided with the end of the free upgrade to Windows 10 and the launch of a dedicated way for customers who use assistive technology to still receive the upgrade for free, which drove significant volumes for support in the first 6 months of FY17.

The average monthly number of customer contacts received by the DAD in FY18 reduced to 16,000. We attribute that decrease to improved online self-help content enabling users to resolve queries without contacting the answers desk. The effectiveness of user support is measured through customer satisfaction surveys following interactions with the DAD, as well as other metrics, including the rate and speed of issue resolution.

In FY19 the average number of customer contacts received by the DAD reduced further to 12,000 per month. Similar to the decrease seen in FY18, this lower number is thanks to the continued improvements being made to the self-help content.

In addition to the DAD and eDAD, our dedicated Accessibility Feedback forum, also known as Microsoft Accessibility UserVoice, allows users to provide accessibility suggestions and feedback on products, features, and tools. Concerns can also be shared by rightsholders through social media inquiries, blog responses, and email.

To better support blind and low vision users, we have partnered with the Be My Eyes app. The free smartphone app, available on iOS and Android, uses video calls to connect around 900,000 people across 150 countries with sighted volunteers to assist with daily tasks and activities. Microsoft is the first technology company to give Be My Eyes a direct route to receive technical assistance through a new Specialized Help
function. Instead of volunteers, customers are connected with a member of Microsoft’s DAD to get support on our products and services. At launch, the service was made available to app users in Australia, Canada, Hong Kong, India, Ireland, Malaysia, New Zealand, the Philippines, Singapore, South Africa, the United Kingdom and the United States.

**Employment**

The ILO Fundamental Principles and Rights at Work and the UN Convention on the Rights of Persons with Disabilities establishes the right of people with disabilities to work on an equal basis with others in a workplace which is inclusive and accessible. Our strategy to respect the rights of people with disabilities includes promoting employment opportunities and career advancement for people with disabilities, within Microsoft and in other employers, through assistance in finding, obtaining, maintaining and returning to employment.

Our [Inclusive Hiring site](#) was launched in FY16 to assist potential candidates with finding job opportunities at Microsoft, including through our Autism Hiring Program. Any role at Microsoft is a potential option for the Autism Hiring Program. Vacancies selected for potential hires with autism are full-time and offer a competitive salary, just like any other job listed on the [Microsoft Careers](#) website.

Resumes are screened for the skills and qualifications necessary in the identified open roles. A set of eligible candidates will be asked to complete an online technical assessment. Candidates may also be invited for a pre-screening interview to gauge their interest, skill and experience for the position. Candidates may then be invited to a multiple-day skills assessment program covering workability, team building, and technical skills at Microsoft’s headquarters. The hiring teams will meet and engage with the candidates during program exercises and job interviews. Based on the skills assessment and hiring manager feedback, the candidate could be offered a full-time job as a Microsoft employee.

The program has led to hiring over 100 individuals in roles including Software Engineer, Service Engineer, Build Engineer, Lab Engineer, Data Analyst or Data Scientist, and other roles in Microsoft, working on products and services like Azure, Cortana, HoloLens, Microsoft IT, Office, Windows, Windows Store and Xbox.
FY19 product accessibility updates

- Xbox Adaptive Controller available at Microsoft Stores
- Accessibility Updates Coming to Windows 10
- New Skype 8.0 Accessibility Improvements
- What’s new with Seeing AI

Society

In FY19, Microsoft continued its support for the human rights work of the G3ict in three important areas related to the digital inclusion of persons with disabilities—smart cities for all, inclusive education and access to justice.

Microsoft collaborated with G3ict’s Smart Cities for All (SC4A), a global initiative to help cities include and empower people with disabilities, to create and pilot G3ict’s Smart City Digital Inclusion Maturity Model. Designed to help city leaders assess how accessible and inclusive for people with disabilities a city’s technology deployments and smart services are, the assessment tool helps city’s track progress and analyze a range of city functions — like communications, training and technology standards — and defines performance indicators and metrics towards expanding accessibility. It can be tailored for a city’s needs and existing infrastructure, and culminates in a confidential report and roadmap for improvement to city officials. Pilot cities included Chicago, Raleigh, North Carolina, Mexico City and Guadalajara.

Microsoft support this year was also critical to G3ict expanding its work in inclusive education and access to justice for people with disabilities. At an event in Kenya, G3ict, with Microsoft and leaders from government and civil society launched new tools developed to help education systems ensure that their technology investments and deployments work for students with disabilities. Like cities and schools, courts and justice systems worldwide are also undergoing a digital transformation. G3ict is spearheading work to understand the role of technology in increasing greater access to justice for people with disabilities. In FY19, Microsoft supported G3ict in expanding the global dialogue on this topic, including through focus groups with courts in both the United States and Mexico.
In Canada, the City of Brampton is working closely with Microsoft Canada to transform experiences for residents and visitors, piloting the Soundscape app. The Soundscape app empowers people with low or no vision to explore the world around them through a 3D audio experience, and is available for free on iOS in both English and French. To ensure Soundscape addresses challenges that Canadians who are blind or have low vision face every day, Microsoft worked closely with the CNIB Foundation and Vision Loss Rehabilitation Canada (VLRC) during beta testing. As Microsoft makes Soundscape available to the public, users are invited to share their experiences through the accessibility UserVoice and can contact the Disability Answer Desk for support.
Data security and privacy

Under Article 12 of the Universal Declaration of Human Rights individuals have a right to be protected from arbitrary, unreasonable or unlawful interference with their privacy, family, home or correspondence. The right is further enshrined in Articles 14 and 17 of the International Covenant on Civil and Political Rights, and other core international human rights instruments. We respect this right by incorporating privacy into design and development processes, offering customers meaningful privacy choices, and by responsibly collecting, managing, and using the customer data that we store.

Approach

Achieving our commitment to rightsholders’ privacy requires a comprehensive privacy program across the company:

- Our Chief Privacy Officer (CPO) works within the Microsoft’s Corporate, External and Legal Affairs (CELA) division, and leads the program. The CPO has global responsibility for Microsoft’s privacy management program, including creating and implementing privacy policy, influencing the creation of privacy technologies and guiding engagement with external stakeholders.
- Our EU Data Protection Officer also sits within the CELA privacy division and oversees personal data processing issues related to Europe.
- Privacy-accountable Corporate Vice Presidents work within Microsoft’s business groups. They interact directly with the CPO, and they bolster the privacy program by overseeing one or more privacy program owners.
- Privacy program owners lead distinct teams of privacy managers embedded within individual products, teams, and groups across Microsoft. These privacy managers are at the heart of the company’s day-to-day privacy work. They conduct privacy reviews of significant new personal data collection and use against a defined set of rules, as set out in the Microsoft Privacy Standard (MPS). The CPO administers the Privacy Management Council (PMC) which is comprised of privacy program owners.

The monitoring, verification and risk assessment of privacy compliance is conducted by three groups at Microsoft:

- The Compliance & Ethics Privacy Compliance Team (CEPC) produces an annual report of privacy governance and compliance, in collaboration with the CPO,
and the report is presented to the Regulatory and Public Policy Committee of the Microsoft Board of Directors.

- Microsoft’s Internal Audit function and the Enterprise Risk Management function also provide regular reporting into the Audit Committee of the Microsoft Board of Directors.

Microsoft engages with a broad array of individuals and groups so that we can identify stakeholder needs and keep pace with changing expectations. These can include governments, regulators, data protection authorities, advocacy groups, academics, and think tanks.

We also participate extensively within industry professional associations, including the International Association of Privacy Professionals (IAPP), and regularly engage with industry partners and peers. There is a regular cadence to these engagements, which is essential for being able to monitor changes in the legal landscape or regulatory and societal concerns.

Microsoft is guided by six privacy principles:

- **Control** – We will put you in control of your privacy with easy-to-use tools and clear choices.
- **Transparency** – We will be transparent about data collection and use so you can make informed decisions.
- **Security** – We will protect the data you entrust to us through strong security and encryption.
- **Strong legal protections** – We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.
- **No content-based targeting** – We will not use your email, chat, files or other personal content to target ads to you.
- **Benefits to you** – When we do collect data, we will use it to benefit you and to make your experiences better.
Policies

We offer two distinct web-platforms to communicate with consumers, or business and enterprise customers, and to provide each group with direct access to their privacy tools.

For consumers, our Privacy at Microsoft website explains our commitment to privacy in plain language. It also provides one single location for consumer users to understand how we respect privacy in our consumer products and services and explains the types of information which Microsoft collects from online browsing and internet searches, geo-location, fitness & health, data used to target ads, sign-in & payment data, information from device sensors, Windows 10 and other online services. The site also contains our layered privacy statement with additional information relevant to particular Microsoft products, and a single location where users can manage their personalization settings, app & services permissions, and marketing & advertising preferences.

Access your privacy dashboard to manage and control your personal data >

To assist our business and enterprise customers, we provide the Microsoft Trust Center, which communicates how we implement and support security, privacy, compliance, and transparency in all our cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud initiative, which explains our guidelines, requirements, and processes for delivering rigorous levels of engineering, legal, and compliance support for our cloud services.

The four pillars of our Trusted Cloud initiative are:

- **Security: Protecting customers from external cyberthreats** – We take customer security very seriously. We spend over a billion dollars a year on our security practices and technologies. Our comprehensive approach to security helps protect customer data wherever it may be – in a datacenter, on a phone, on a desktop, or in transit through the Internet. Learn more >

- **Privacy and control: Giving customers control over access to their data** – At Microsoft, we fundamentally believe that customers’ data is their own data, whether it sits in our cloud or in their own datacenter. We invest heavily in
technology development and practices to ensure we actively protect privacy and provide the necessary tools to control both the privacy and administrative aspects of the data put in the Microsoft Cloud. Learn more >

- **Compliance: Unparalleled investment in meeting global standards** – Our extensive experience working with the world’s largest governments and enterprises in the most highly regulated industries has been transferred to our cloud services. Our investments in compliance-related technology, resources and staff help ensure that we are proactively adopting new certifications and partnering with regulators and standards bodies to develop new regulation and standards when we identify opportunities to increase digital privacy and safety. Learn more >

- **Transparency: Clear insight into our policies and procedures** – Transparency plays an important role in developing trust – we work tirelessly to increase not only our own transparency, but the transparency of the industry and its regulators. We publish reports detailing government requests for customer data. We notify individual customers when the government requests data from their data or applications when legally allowed to do so. Finally, we submit to a set of third-party audits and publish the results for our customers. Learn more >

**Actions**

In our previous human rights reports we have covered our efforts to prepare for and then launch our compliance with the European Union’s (EU) General Data Protection Regulation (GDPR). The GDPR applies to companies and individuals in the EU, as well as organizations outside of the EU if they collect or process personal data of EU residents. The Regulation has nearly 160 requirements covering how companies collect, store and use personal information, and it requires notification for personal data breaches within 72-hours. The GDPR builds on article 8 of the European Convention on Human Rights, which establishes that everyone has the right to protection of private and family life, in home and in correspondence.

Significantly, the GDPR elevates and clarifies existing requirements to enable individuals to access, control, correct and delete data. Additionally, the GDPR creates new requirements regarding the portability of data, and the level of transparency that must be provided in association with certain algorithmically determined decisions. After years of debate and preparation since it was first proposed in 2012, the GDPR came into effect on May 25th, 2018. The introduction of the GDPR has also inspired countries around the world to adopt new privacy laws that are modeled on GDPR. Brazil, China,
India, Japan, South Korea and Thailand are among the nations that have passed new laws, proposed new legislation, or are considering changes to existing laws that will bring their privacy regulations into closer alignment with the GDPR.

The GDPR required that we update our existing privacy standards and execute on our standards at a larger scale than ever before. We launched a companywide initiative called Next Generation Privacy (NGP). Our NGP initiative provides a comprehensive framework that includes policies, processes, technical infrastructure, and customer experiences to address privacy at all levels of our organization and deliver the standardization needed for compliance. Within this framework, we identified accountable executives in each of our engineering, business, and specialized organizations who have day-to-day responsibility for GDPR compliance in their group.

Our philosophy towards privacy and compliance remains the same – we view privacy as a fundamental right and we are committed to complying with privacy laws and regulations. We have been advocating for national privacy legislation in the United States since 2005 and we have been enthusiastic supporters of the GDPR since it was first proposed. We also believe new rights at the heart of the GDPR establish important principles that are equally relevant outside the EU. Called “Data Subject Rights,” they include the right to know what data is collected, to correct that data, and to delete it or move it to a different place.

When the GDPR went into effect in May 2018, Microsoft announced that it would be the first company to extend Data Subject Rights to all of our consumer customers around the world. This wasn’t required by GDPR, but we chose to do it because we firmly believe that helping put people in control of their data is the right thing to do. To achieve that goal, we built a privacy dashboard where our customers can manage their privacy settings, see what data we have stored, and delete that data if they want to. This includes everything from browsing and search history to location activity, movies and TV viewed through a Microsoft app or service, and health data in Microsoft Health.

In the first four months more than 5 million people from over 200 countries logged onto the Microsoft privacy dashboard to manage their information. It has been striking to see the strong interest and engagement from around the world. The highest level of engagement came from U.S. customers with approximately 2 million people using our privacy dashboard to manage their data. Also included in the top 10 countries for visits
on a per capita basis were Japan, with nearly 400,000; Brazil, with over 200,000; and China and Mexico, each with over 135,000 customers logging on to manage their data.

After 12 months more than 18 million people from around the world have used our tool to manage their personal information. The highest level of engagement, both on a per capita basis and in absolute numbers, continued to come from the United States where about 6.7 million people have used the dashboard. Not surprisingly, residents of European countries covered under GDPR also account for a significant percentage of people who have visited the privacy dashboard—to date more than 4 million of our customers in the EU have logged on to manage their data. By May 2019 the top 20 countries using the privacy dashboard were:

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of users</th>
<th>Country</th>
<th>Number of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. United States</td>
<td>6.7 million</td>
<td>11. Italy</td>
<td>315,000</td>
</tr>
<tr>
<td>2. Japan</td>
<td>1.4 million</td>
<td>12. Spain</td>
<td>292,000</td>
</tr>
<tr>
<td>3. United Kingdom</td>
<td>1.3 million</td>
<td>13. Netherlands</td>
<td>271,000</td>
</tr>
<tr>
<td>4. France</td>
<td>807,000</td>
<td>14. India</td>
<td>269,000</td>
</tr>
<tr>
<td>5. Canada</td>
<td>726,000</td>
<td>15. South Korea</td>
<td>217,000</td>
</tr>
<tr>
<td>6. Brazil</td>
<td>673,000</td>
<td>16. Turkey</td>
<td>188,000</td>
</tr>
<tr>
<td>7. Germany</td>
<td>615,000</td>
<td>17. Russia</td>
<td>172,000</td>
</tr>
<tr>
<td>8. China</td>
<td>435,000</td>
<td>18. Belgium</td>
<td>163,000</td>
</tr>
<tr>
<td>9. Mexico</td>
<td>384,000</td>
<td>19. Colombia</td>
<td>145,000</td>
</tr>
<tr>
<td>10. Australia</td>
<td>378,000</td>
<td>20. Sweden</td>
<td>135,000</td>
</tr>
</tbody>
</table>

The information from our privacy dashboard tells us two important and related things:

- First, there is a high level of interest among consumers around the globe in having control over their personal data.
- Second, American consumers are no exception, as they are actively engaging with control tools they are provided. This fact puts to rest the notion that Americans care less about their privacy than Europeans. It also lends greater urgency to the need for federal legislation that provides tools and protections that make it easier for American consumers to exercise control over their personal data throughout the ecosystem.
To help bring extra legislative protection to users in the US, we supported efforts by the Washington State legislature to pass Senate Bill 5376, the Washington Privacy Act (WPA). This landmark legislation would have provided consumers in Washington state with the strongest set of privacy protections in the United States. It ensured that consumers, and not businesses, retain control over their personal information online. It gave consumers the right to opt out so that their personal data is not sold, shared or used for advertising, while also holding businesses responsible for safeguarding personal information, and it authorized Washington state’s attorney general to prosecute businesses for privacy violations and impose civil penalties.

The bill was an ambitious and bold proposal; for the first time, it would have provided US consumers with consumer rights and held companies accountable for their data practices – provisions that were inspired by the GDPR.

After passing out of the Senate with a broad, bipartisan vote of 46-1, the House failed to act before the session ended. While we are disappointed and believe this was a missed opportunity, we remain committed to working with all stakeholders to bring broad, robust privacy protections to life in the United States, including in Washington state, and we continue to advocate for the US Congress to enact legislation that extends privacy protections in the GDPR to citizens in the US.

Also in FY19 we announced major steps to increase transparency about the data we collect when people use our products and to provide them with greater control over how their data is used. Those steps include describing the data we collect in clear and simple language, and in all our major products we’ll categorize the data we collect from devices as either required or optional. In some cases, a customer can control whether required data is collected by deciding whether to use the product features or functions that depend on that required data.

To enhance transparency reporting, we are improving documentation and introducing a new biannual report about our data collection procedures. We’ll improve upon our existing documentation practices to describe what we collect in these two categories in ways that are easy to understand, and to explain why data in the required category is necessary. And we will consolidate and present this information to make it easier to find. All customers will be able to access this information through our privacy.microsoft.com hub, or in our enterprise Trust Center. The new biannual report will highlight any new required data collection we believe is fundamental to provide,
secure, update or maintain the performance of our products. We will also note instances when we stop collecting certain types of data from devices (because product or service changes mean the data is no longer required). Last, we will explain when we make changes to our data collection in response to new privacy laws, industry standards and regulations.

We have also delivered features that improve how businesses secure sensitive data and protect the privacy of their employees and customers. We offer encryption to enable companies to protect sensitive data including credit cards and national IDs such as US Social Security numbers. To help companies safeguard sensitive information on mobile devices, we announced a set of advanced privacy and security capabilities that enable companies’ IT administrators to better enforce privacy and security protection policies. And in April, we released new privacy tools for Office365 ProPlus that provide greater control over diagnostic data that is sent to Microsoft, and over optional cloud-based features in Office that enhance functionality.

Finally, we continue to provide users with a direct reporting mechanism through which they can request data access and deletion, and to make choices about Microsoft’s collection and use of their data by visiting the How to Access & Control Your Personal Data section of our Privacy Statement. Trained professionals oversee and process user submissions daily, and they have an escalation channel to the CPO’s team.

Customers can also use the Microsoft Privacy Support Form to raise questions or feedback around Microsoft’s privacy practices. Customer inquiries raised through the Privacy Support Form are incredibly valuable in helping to improve our customer experiences and to help ensure we are living up to our Privacy Principles.

When a customer submits a question to privacy support, that case is routed centrally through the office of the Chief Privacy Officer. Inquiries span almost all of Microsoft’s products or services and the privacy team can follow up with the product groups when necessary to help resolve the issue. Changes are made to our products to respond to customers’ requests. These actions directly support our first and second privacy principles on control and transparency.
Microsoft privacy support responded to close to 10,000 customer inquiries in FY16, and close to 4,000 customer inquiries in both FY17 and FY18, thanks to improved controls on the privacy dashboard. In FY19, there was a notable increase in the number of queries and requests in the months surrounding the introduction of the GDPR. We received 21,000 submissions. Many of those inquiries were from commercial customers working towards their own compliance. The US still submitted the majority of inquiries.
Freedom of expression and privacy

Respecting peoples’ rights to freedom of expression and freedom from arbitrary or unlawful interference is enshrined in multiple articles in the International Covenant on Civil and Political Rights. Article 17 establishes that no one shall be subjected to arbitrary or unlawful interference with their privacy; Article 19 affirms that everyone shall have the right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers; and Article 20 requires that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law. Exercising the rights to freedom of expression and privacy online is essential to the enjoyment of other human rights which are fundamental pillars for democracy and good governance.

Policies

To meet our commitments to the freedom of expression and privacy rights of our users, Microsoft supports the rule of law that meets international norms and standards, including internationally recognized human rights laws and standards. Accordingly, we advocate the following principles:

- In regulating online content, conducting surveillance or accessing data, governments should fully commit to the rule of law. This means ensuring that laws and regulations, including their enactment and enforcement, are transparent and respect international human rights laws and norms. Rule of law requires that government orders and decisions should be subject to independent judicial approval and review, with meaningful and trusted opportunity for companies and individuals to appeal judicial approvals or decisions. Laws and regulations should not restrict companies from informing the public about demands from governmental authorities for content removal or access to data.
- Government restrictions to online content must be governed by clear rules that are necessary and proportionate, protective of people's rights to share even unpopular ideas, enforced in a transparent manner and without discrimination. Legal orders for the removal of illegal content must be specific, narrowly tailored, and sufficiently detailed to enable companies to identify precisely which content must be taken down.
- Government orders for access to user data must name the specific user account or identifier, and whenever possible should be directed at the customer itself, or
if issuing the order directly to the customer is inappropriate (e.g., imperil an ongoing investigation or result in further danger to public safety), then at the entity most directly involved in providing the service to the customer.

- Except in limited cases, individuals and organizations have a right to know when governments access their digital information. Governments must provide case-specific facts to seek judicial or other independent approval of restrictions on the service provider’s ability to notify its customers of government orders for customers’ data, and the restrictions must be limited in duration and scope to that which is necessary to serve law enforcement’s demonstrated need for secrecy.

- Although the global internet is borderless, governments should respect international borders and the sovereignty and laws of other nations, and they should agree upon a framework for requesting data stored outside its borders that avoids and resolves conflict of laws and protects privacy and human rights.

- Service providers must receive detailed legal process from law enforcement to allow for thorough review of the demand for user data, and must also have clear mechanisms to challenge unlawful and inappropriate demands for user data to protect human rights.

The Microsoft Human Rights team leads and works across the company to develop and implement policies and practices to meet Microsoft’s commitment to freedom of expression, privacy and other human rights, and to engage external stakeholders on the advancement of and policy advocacy for those rights.

Implementing these principles requires consistent processes:

- **Freedom of Expression** – Microsoft has internal processes and procedures to document and address government requests for content removal or user data, which enables us to meet our commitments to respect the freedom of expression and privacy rights of our users.

When Microsoft receives a government request to remove content we carefully review and assess the demand to understand the reason for the request, the authority of the requesting party, the applicable internal policies or terms of use for the affected product or service, and our commitments to our customers and users including with regard to freedom of expression. Based on these reviews, we determine whether and to what extent we should remove the content in question.
Privacy – Microsoft adheres to the same principles for all requests from government agencies for user data, requiring governmental entities to follow the applicable laws, rules and procedures for requesting customer data. We do not provide any government with direct and unfettered access to our customers’ data, and we do not provide any government with our encryption keys or the ability to break our encryption.

If a government wants customer data, it needs to follow applicable legal process, meaning, it must serve us with a warrant or court order for content or a subpoena for subscriber information or other non-content data. We require that any requests be targeted at specific accounts and identifiers. Microsoft’s compliance team reviews government demands for user data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order.

We make clear the relevance and significance of these issues and policies in several ways. We make public commitments to respect the freedom of expression and privacy rights of our users via the Microsoft Global Human Rights Statement. We engage with stakeholders including:

- The Global Network Initiative (GNI), which is a multi-stakeholder organization of technology companies, civil society, academic institutions and investors with a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector.
- Governments around the world.
- International organizations.

Actions
To help stakeholders evaluate how we are meeting our commitments to freedom of expression and privacy we produce several disclosures twice per year. Individual reports are available for:

- Content Removal Requests
- Law Enforcement Requests
- US National Security Orders
These Digital Trust Reports are a key component to our commitment to be transparent about governments' requests to access data or remove content. In addition to providing external transparency, the reports are also another step we take to communicate to our employees that the respect of the freedom of expression and privacy rights of our users is the responsibility of every employee, and we have internal teams that are focused on supporting employees across the company to meet that responsibility.

As a member of GNI, Microsoft participates in the GNI Independent Assessment Process. Our FY17 human rights report covered the GNI’s Public Report on the 2015/16 Independent Company Assessments which noted our “commitment to protecting freedom of expression and privacy genuinely seems to have become a ‘lens’ through which business decisions are evaluated at various levels of the company.” That was the second independent assessment, and it once again determined that Microsoft complies with the GNI Principles on freedom of expression and privacy.

In FY19, Microsoft completed its third GNI assessment by an independent assessor. After reviewing the assessment report by the independent assessor and discussing the report with the assessor and Microsoft, the GNI Board concluded that Microsoft continues to make good faith efforts to implement, and with improvement over time, the GNI Principles on freedom of expression and privacy. We will issue a fuller statement in early 2020 following the release of the formal GNI report on the 2019 assessments of GNI companies.

View more information on the GNI company assessments >
Online safety

Providing tools and resources to protect the safety and security of all online users is a core component to meeting our responsibility to respect Universal Declaration of Human Rights, Article 2; Individuals have a right to not be discriminated against, directly or indirectly, on various grounds, including race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. By upholding the Code of Conduct section within the Microsoft Services Agreement, rightsholders are equally empowered to exercise their rights online through a safe and inclusive Internet.

Approach

The dual-use nature of Internet technologies requires Microsoft to both limit certain behaviors and encourage others. We use a complementary approach of encouraging safe behaviors online by directly implementing efforts and engaging in partnerships to foster civil interactions, and by offering tools and resources so that users can empower themselves. The Microsoft Services Agreement (MSA) is the foundation of our approach to promoting online safety. The MSA’s Code of Conduct outlines the acceptable behaviors in our online services. Dedicated complaint-response teams are responsible for enforcing the Code's provisions on all our hosted consumer services, for example OneDrive, Skype and Xbox Live.

Microsoft’s Digital Safety team is responsible for all aspects of our online safety strategy, including cross-company policy creation and implementation, influence over consumer safety features and functionality and communications to, and engagement with, a variety of external audiences. This approach to online safety is best reflected in our four-part strategy:

- **Technology** – Strive for simple, easy-to-use products and services that are built with safety, security, and privacy in mind at the earliest stages of the development process.

- **Governance** – Devise and grow an internal self-governance program with policies, standards and procedures for addressing various customer-use and abuse scenarios.
**Awareness raising** – Inform the public about existing and emerging risks. Share resources and ways in which individuals and families can protect themselves online.

**Partnerships** – Work with others in the technology industry, civil society, academia and government, as no one organization or entity can tackle these significant, novel and nuanced issues alone.

**Policies**
The MSA became effective in September 2016. The MSA is a unified term of use to replace the previous, separate terms such as the “Xbox Live Terms of Use” or the “Skype Terms of Use”. The MSA was most recently updated on July 1, 2019.

Individual users accept the terms of the agreement whenever they create a Microsoft account or a Skype account, or when they use Microsoft services, or if they continue to use our services after being notified of changes within the terms. The products, apps and services covered by the MSA are listed within the agreement.

The Code of Conduct within the MSA prohibits certain online behaviors. The Code is enforced through multiple procedures, including by professionally trained teams specializing in content moderation to implement our policy. The teams are responsible for receiving and processing cases received from customers, governments, and other groups.

When necessary, the team can stop users who do not abide by the Code of Conduct from receiving access to Microsoft services. The team can also block the delivery of emails, instant messages and other communications to and from Microsoft services, and Microsoft can deny access to content.

Read the Microsoft Services Agreement and its Code of Conduct >

**Public safety**
In our human rights report for FY16 we reported on our new terrorist content approach which specifically prohibits the posting of terrorist content on our hosted consumer services. We consider terrorist content to be material posted by or in support of a terrorist or terrorist organization on the Consolidated United Nations Security Council.
Sanctions List that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.

Our terrorist content approach continues our “notice-and-takedown” process for removal of prohibited – including terrorist – content from our hosted services when it is brought to our attention via a dedicated web-reporting form. All reporting of terrorist content – from governments, concerned citizens or other groups – on any Microsoft service should be reported to us via this form.

In our human rights report for FY17 we also reported on the formation of the Global Internet Forum to Counter Terrorism (GIFCT). The Forum’s mission “is to substantially disrupt terrorists’ ability to use the internet in furthering their causes, while also respecting human rights. This disruption includes addressing the promotion of terrorism, dissemination of propaganda and the exploitation of real-world events through online platforms.” The Forum uses a three-prong strategy:

- Employing and leveraging technology
- Sharing knowledge, information and best practices
- Conducting and funding research

The March 2019 terrorist attack against two mosques in Christchurch made it clear that across the tech sector we need to do more. That month, we outlined some of the actions we would take going forward:

- Focus on prevention
- Respond more effectively to moments of crisis
- Foster a healthier online environment more broadly

In May 2019 the New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron brought together government leaders and representatives of technology companies to announce the “Christchurch Call to Action To Eliminate Terrorist and Violent Extremist Content Online.” In response to the Call, Amazon, Facebook, Google, Twitter and Microsoft issued a joint statement.

The companies also published nine steps they’ll take to address the abuse of technology to spread terrorist and violent extremist content. These nine steps include
five individual actions that each company is committing to take, and a further four collaborative actions they’ll take together.

The five individual actions for the online content sharing service providers to address the abuse of technology to spread terrorist and violent extremist content cover:

- Terms of use
- User reporting of terrorist and violent extremist content
- Enhancing technology
- Livestreaming
- Transparency reports

The four collaborative actions include:

- Shared technology development
- Crisis protocols
- Education
- Combatting hate and bigotry

Youth empowerment

We launched a Council for Digital Good in FY17. The Council is an important part of our continuing efforts to promote online safety for youth. The Council consists of 15 young people from across the US and they meet to help teens and others fully appreciate and understand the risks and potential harms associated with life online.

The Council’s inaugural summit was held in August 2017. The members identified five key areas of concern:

- Self-obsession and the need to constantly post and share personal information
- “Addiction” to screens, connectedness, likes and followers
- Social posturing to frame one’s online image as positive, provocative, exciting or enviable
- A lack of authenticity and transparency that inhibits individuals from being their true selves online
- The prevalence of online hate
The Council sent an open letter to US law- and policy-makers in July 2018 calling on government to address digital-world realities like cyberbullying and “sextortion” by modernizing laws and promoting in-school education to encourage positive online behaviors.

The letter was also shared at an event featuring the 15 members at Microsoft’s Innovation and Policy Center in Washington, DC. The letter highlights the benefits of awareness-raising of digital risks, as well as recommending that in-school online safety and behavioral education be supported and prioritized, and makes a request that laws be updated and brought into the digital age. This letter and its recommendations to policymakers represent a culmination of the council’s work after 18 months of other assignments, activities, learning and fun. In addition to the council members and a parent or chaperone who accompanied each of them to the event, the young people also hosted leaders from other technology companies, non-governmental organizations and DC-area influential individuals.

This inaugural pilot program formally concluded following the DC event. Many of the individual council members are joining other organizations to continue to learn, grow and advocate for these critical societal issues.

Other Council for Digital Good-related activities are underway, including with Microsoft Egypt spearheading the formation of an African Council for Digital Good as well as an Arab Council for Digital Good. Nearly 750 applicants across both regions vied for 24 positions on the two councils. We look forward to the work of these two new councils and the impact these teens will have in promoting digital civility in their regions and around the world.

In our FY17 human rights report we shared efforts to help to grow the evidence base for online safety with unique research focusing on digital civility. Our research is intended to shine a light on the online challenges faced by people around the world and to encourage everyone to treat each other with dignity and respect.
Findings from our first year of research were released on Safer Internet Day 2017 and included our Digital Civility Index. Teens aged 13-17 and adults aged 18-74 were surveyed in 14 countries to gauge their perceptions of digital civility across 17 online risks in four categories: behavioral, reputational, sexual and personal / intrusive. Two out of 3 respondents reported having been victim of at least one risk, and 50% reported that they were “extremely or very” worried about online life in general.

To mark World Kindness Day 2017, we released additional findings to emphasize how online users are helping to foster safer, healthier and more respectful online interactions. Eighty-eight percent of teens and 87% of adults said they treat other people with respect and dignity online, and 84% of both teens and adults reported that they show respect for other peoples’ points of view. Importantly, 65% of teens and 59% of adults responded that they stand up for others online.

The findings from the second year of digital civility research were released in FY18. The number of risks being assessed increased to 20 from 17, and the study expanded to 23 countries, up from 14 countries in 2016, and included separate regional reports for both Asia and Latin America. “Unwanted contact” was identified as the top risks, with 41% of respondents reporting that they had been contacted online by someone they did not wish to hear from. This is down 2% points from 43% in the previous year’s survey.

Findings from the third year of the study, released in FY19, showed that teenagers around the world are increasingly turning to their parents and other trusted adults for help with online problems. 42% of teens from 22 countries who encountered online issues said they asked their parents for help, while 28% said they sought advice from another adult such as a teacher, coach or counselor. Those figures are up an impressive 32% and 19%, respectively, compared to the previous year’s findings which showed only 10% of young people turned to their parents for advice and just 9% asked for help from other adults. In addition, adults and teens across the globe say parents are by far the best placed of any group to keep young people and families safe online. Results show parents have both the greatest potential — and were deemed the most effective — at promoting online safety among young people, teens and families.

Teenage girls were more likely to ask for help from their parents - 44% of girls vs. 37% of boys, and from other trusted adults - 29% of girls vs. 26% of boys, which is likely because life online in general is harder on girls than boys. The data demonstrates that
girls have a higher level of online risk exposure than boys; they suffer more consequences and “pain” from online ills, and the online risks and abuse that they experience are more emotionally charged. Moreover, as online risks have grown in severity — for example “sextortion” and “swatting” — young people are perhaps more inclined to seek advice from the older generation. 66% of female teenage respondents reported being exposed to online risks vs. 60% of male teenage respondents. Furthermore, 73% of girls reported negative consequences following an online issue compared to 67% of boys, and the level of pain associated with online risks and the intensity of the attendant emotions — namely fear, anger and sadness — were higher for girls.

In general, millennials around the world — those between the ages of 18 and 34 — are exposed to the highest levels of online risk and suffer the most severe consequences from those risks when compared to other age groups. In addition, once millennials have had a negative experience online, more so than other age groups they lose trust in others online and off; they become stressed, depressed, lose sleep or lose a friend; and they worry that the hurtful experience will happen again.

The research also found that online social circles are becoming riskier. Bullying, unwanted contact and receiving unwelcome sexual images and messages were the most prominent risks and, while strangers still pose the majority of online threats, data shows a distinct rise in risk-exposure from people’s own social circles.

63% of online risks came from strangers and people whom respondents knew only online – largely unchanged from the previous year. Meanwhile, 28% of online risks came from family and friends, up 11 points. In addition, findings revealed a relationship between risk-exposure and familiarity with the perpetrator: respondents who had met their abuser in real life were almost twice as likely to experience an online risk. More disheartening were indications that people were targeted because of their personal characteristics, namely gender, age and physical appearance.

Discover how to promote digital civility and more detail from Digital Civility Index >
Sustainable Development Goals

The success of the Sustainable Developments Goals (SDGs) requires action and collaboration by all actors, and the SDGs explicitly call on all businesses to contribute creativity and innovation to solve sustainability challenges.

The SDGs are an ambitious global agenda for the development of all countries. The SDGs were formed through consultations and negotiations led by the UN and have been agreed to by all governments to create a 15-year global roadmap to create sustainable societies, economies and ecosystems by eliminating poverty, promoting prosperity and protecting the environment. If successful, the SDGs will build a life of dignity and opportunity for all, while safeguarding the ability of future generations to achieve the same.

Technology is increasingly an essential gateway to the exercise of human rights, and we are working to foster a sustainable future where everyone has access to the benefits it provides. Our commitment is reflected in how we apply our technology, talent, and financial resources to foster opportunity and serve the needs of communities around the globe, and is reflected in our corporate social responsibility's three key pillars: empowering people, strengthening communities and protecting the planet.

The Danish Institute for Human Rights has published a Human Rights Guide to the SDGs. The Guide connects human rights instruments, and individual articles within those instruments, to all goals and targets of the SDGs. We use that guide here to provide an illustrative, but not exhaustive, list of how our efforts to respect the human rights salient to Microsoft’ business may contribute to achieving the SDGs.
<table>
<thead>
<tr>
<th>Salient human rights issue</th>
<th>Key human rights instruments and articles</th>
<th>Key SDGs</th>
<th>Key SDG targets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accessibility</strong></td>
<td>Universal Declaration of Human Rights – Article 2</td>
<td>SDG 10 – Reduce inequalities</td>
<td>10.2 - By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status.</td>
</tr>
<tr>
<td></td>
<td>Convention on the Rights of People with Disabilities – Article 9</td>
<td>SDG 12 – Responsible consumption and production</td>
<td>12.8 - By 2030, ensure that people everywhere have the relevant information and awareness for sustainable development and lifestyles in harmony with nature.</td>
</tr>
<tr>
<td><strong>Data security and privacy</strong></td>
<td>Universal Declaration of Human Rights – Article 12</td>
<td>SDG 16 – Peace, justice and strong institutions</td>
<td>16.10 - Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements.</td>
</tr>
<tr>
<td></td>
<td>International Covenant on Civil and Political Rights – Article 17</td>
<td>SDG 16 – Peace, justice and strong institutions</td>
<td>16.10 - Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements.</td>
</tr>
<tr>
<td><strong>Freedom of expression and privacy</strong></td>
<td>Universal Declaration of Human Rights – Article 19</td>
<td>SDG 16 – Peace, justice and strong institutions</td>
<td>16.10 - Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements.</td>
</tr>
<tr>
<td></td>
<td>International Covenant on Civil and Political Rights – Article 19</td>
<td>SDG 16 – Peace, justice and strong institutions</td>
<td>16.10 - Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements.</td>
</tr>
<tr>
<td><strong>Online safety</strong></td>
<td>Universal Declaration of Human Rights – Article 2</td>
<td>SDG 10 – Reduce inequalities</td>
<td>10.2 - By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status.</td>
</tr>
</tbody>
</table>
### Glossary of abbreviations and technical terms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>CPO</td>
<td>Chief Privacy Officer</td>
</tr>
<tr>
<td>DAD</td>
<td>Consumer Disability Answers Desk</td>
</tr>
<tr>
<td>eDAD</td>
<td>Enterprise Disability Answers Desk</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>G3ICT</td>
<td>Global Initiative for Inclusive Information and Communications Technology</td>
</tr>
<tr>
<td>GIFCT</td>
<td>Global Internet Forum to Counter Terrorism</td>
</tr>
<tr>
<td>GNI</td>
<td>Global Network Initiative</td>
</tr>
<tr>
<td>IAPP</td>
<td>International Association of Privacy Professionals</td>
</tr>
<tr>
<td>MAS</td>
<td>Microsoft Accessibility Standard</td>
</tr>
<tr>
<td>MPS</td>
<td>Microsoft Privacy Standard</td>
</tr>
<tr>
<td>MSA</td>
<td>Microsoft Services Agreement</td>
</tr>
<tr>
<td>NGP</td>
<td>Next Generation Privacy</td>
</tr>
<tr>
<td>OHCHR</td>
<td>Office of the High Commissioner for Human Rights</td>
</tr>
<tr>
<td>SC4A</td>
<td>Smart Cities for All</td>
</tr>
<tr>
<td>SDGS</td>
<td>Sustainable Development Goals</td>
</tr>
</tbody>
</table>