Cisco Human Rights Position Statements

Introduction

A variety of disruptive technologies and trends are shaping our future, and in doing so will transform the business and human rights landscape. For example, artificial intelligence (AI), big data analytics, and the internet of things (IoT) all have the potential to address humanity's most pressing challenges, such as those relating to accessibility, health care, education, transportation, counter-terrorism, and criminal justice. However, these disruptive technologies and trends also bring new and previously unforeseen human rights risks as diverse as non-discrimination, privacy, child rights, security, freedom of expression, and access to employment, housing, credit, and public services.

These developments are relevant across Cisco's value chain, including our supply chain, our own operations, and the use of our products, services, and technologies by our customers. In accordance with our Human Rights Policy, we are committed to identifying these human rights impacts, mitigating risks, maximizing opportunities, and fostering collaborative and transparent engagement with our stakeholders. This document describes the relevance of disruptive technologies and trends for human rights at Cisco and sets out our significant activities and point of view for each.

- Encryption
- Data localization and sovereignty
- Surveillance by governments
- Internet of things
- Big data analytics
- Artificial intelligence

Encryption

CONTEXT/TECHNOLOGY

Data encryption is an essential part of protecting information. In the digital age, data breaches, malware, and other security threats have put at risk the vast amounts of personal data (emails, messages, health records, credit card information, etc.) that are shared or stored via the internet daily. Encryption helps to safeguard our online information and activities—providing security of user data, authentication, confidentiality, and consumer trust—and creates new opportunities for communication and expression. Strong encryption also helps ensure that critical systems—such as those delivering water, food, healthcare, transportation, telecommunications, and energy—are secured against interruptions and attacks.

HUMAN RIGHTS IMPACTS

Encryption is crucial in helping people exercise certain human rights, such as the right to privacy and freedom of expression. These, in turn, can be necessary for exercising other rights such as freedom of association and assembly and the right to life and bodily integrity.

For certain individuals, such as political activists, human rights defenders, and other vulnerable groups, encryption can help protect against surveillance and arbitrary interception of communications by governments. In some cases, governments will attempt to weaken or circumvent encryption by requesting encryption keys and backdoors. These efforts have serious consequences for the security and privacy of users.

Encryption makes it harder for hackers and criminals to access private data; however, law enforcement agencies are concerned that encryption makes it more difficult to prevent crime (including human rights abuses, such as human and sex trafficking), and protect national security. Developing a holistic security approach so it addresses both individual security risks (safeguarding an individual at risk or identifying an individual bad actor) and infrastructure security risks (cybersecurity and network defense) is an important responsibility shared across multiple stakeholders.

CISCO RELEVANCE AND APPROACH

Data protection is part of Cisco's DNA. We build data protection and encryption into our culture through our policies, processes, technology, and people interactions. This helps us avoid the risks of bad behaviors or breaches, and ensures employees know that protecting Cisco data is everyone's responsibility. We make extensive, even mandatory use of encryption to protect customer data that we handle, and our products enable customers to use encryption.

Our Product Security Baseline provide internal security-related requirements for our products and have minimum requirements around credential and key management, cryptography standards, anti-spoofing capabilities, integrity and tamper protection, and session/data/stream management and administration. We have also established a repeatable and measurable process, the Cisco Secure Development Lifecycle, which reduces the number and severity of vulnerabilities in software.

We also use Privacy Engineering to develop technology solutions that preserve and protect information and ensure authorized use throughout the lifecycles of our solutions and offerings. Our Privacy Data Sheets describe the processing of personal data for various products, including how we use encryption to secure data in transit and at rest.

Cisco's Trust Center provides a comprehensive view of how we deal with data protection and privacy issues. Our Trust Principles express our commitment to maintaining strong protections for our customers, products and company, and provide the foundation for how we develop products and engage with customers.

CISCO POINT OF VIEW

We believe security and privacy are not mutually exclusive—and are often dependent on one another.

We have a responsibility to provide secure services to our customers without backdoors, which we define as any surveillance capability that is intentionally created by not transparently disclosed. We oppose backdoors and believe that any backdoor or weakening of a cryptographic system is a vulnerability available to a potential bad actor. We do not deliberately build backdoors into our products, and we do not knowingly enable backdoors in our products.

To the extent that governments demand the creation of a new surveillance capability while simultaneously preventing the public documentation of the existence of that capability, they are creating a new backdoor. For this reason, we oppose attempts to prohibit public disclosure about new surveillance capabilities demanded by governments.

We believe governments should turn over security vulnerabilities known to them promptly when found, apart from limited duration exceptions by court order for exigent purposes involving saving lives and national security. We believe that governments should deploy transparent processes for vulnerability handling, reporting, and disclosure that are subject to meaningful oversight. It should not be a matter of "if" governments are required to notify vendors of vulnerabilities, but "how long" until governments notify them. The processes in place to govern vulnerability handling must strike a balance between safety and security in exigent circumstances and securing systems against attacks more broadly.

We believe there is an urgent need for greater consensus among governments, law enforcement agencies, civil society groups, human rights defenders, and companies on the setting of norms to govern the way forward. We will participate as an engaged and constructive stakeholder in—and are actively funding civil society efforts to establish—dialogue about how governments and law enforcement agencies can achieve legitimate objectives without recourse to backdoors or overbroad requests, especially in the areas of serious crime, national security, and counter-terrorism.

When we ourselves learn of a security vulnerability in a product or service, we respond by validating it, fixing it, and informing our customers. If a customer's security has been impacted by external forces, we react the same way, regardless of the origin of the security breach. We do so in accordance with ISO standards by making risk-based determinations about whether and how to fix the security vulnerability.

Data Localization and Sovereignty

CONTEXT/TECHNOLOGY

As communication systems and the internet have broken down geographical barriers, so data flows across borders have increased significantly. In response, some countries have responded with measures requiring the retention of data within their borders. Data localization policies require certain types of data to be stored on local servers, and data sovereignty comes into play when such data is subject to the laws or legal jurisdiction of the country in which it is stored.

These limitations can prove to be a challenge for companies as law enforcement, privacy, and data sovereignty regulations vary from country to country. In addition, the nature of communications systems today is such that storing data in only one jurisdiction may not always be technically feasible; international data flows are disrupting traditional notions of jurisdiction, sovereignty, and national boundaries.

HUMAN RIGHTS IMPACTS

Data localization policies are often touted as providing data protection and privacy benefits for citizens' personal information, but the real situation is more nuanced. For example, data sovereignty requirements may prevent sensitive health information from one country being processed in another jurisdiction with weaker privacy protections—however, data sovereignty requirements can also limit and restrict data flows that could be important for making a crucial health decision. In addition, localization requirements can provide a false security, in that security vulnerabilities can exist regardless of where data is stored, and the largest threat may not be that data are in a different country.

Data localization policies can also be an attempt for governments to exercise greater control over their citizens, and present significant risks to human rights when mandated by governments with inadequate respect for rule of law and human rights protections. In these circumstances data localization requirements can increase risks to privacy, security, and freedom of expression, especially for vulnerable groups.

CISCO RELEVANCE AND APPROACH

Cisco collects and processes data across our wide-range of products and services. We inventory and map the data that we process, including our cloud-based products and services. This is key to managing data appropriately and consistently as it helps us understand what data we have, how we are protecting it, what we are doing with it, where it is, where it flows, who has access to it, and why.

We have updated our privacy and data protection policies and internal standards and governance with clear rules on how we process personal data, including our efforts to comply with GDPR requirements in the EU and the California Consumer Privacy Act, for example. Our Privacy Statement has a section on our approach to safeguarding personal information—making it clear to customers and users how their data might be transferred, processed, and stored.

CISCO POINT OF VIEW

Cisco is committed to helping our customers and partners by protecting and respecting personal data, no matter where it comes from or where it flows.

Cisco believes that customers and clients, not governments, should determine where their data is stored and how it is processed, and for this reason we do not support government mandates for data localization and data sovereignty requirements. We believe that governments should respect international borders and the sovereignty of other nations in matters of data and privacy. In cases where governments seek to compel data from foreign storage locations, we believe governments should be expected to use the proper channels, such as mutual legal assistance treaties.

We believe that countries and law enforcement agencies should establish clear, predictable, and rational requirements for cross-border data demands, including clarity on potential conflicts of law with third countries. We further believe that countries should agree equivalent levels of substantive and procedural protections for privacy, civil liberties, and human rights when sharing data. These arrangements would reduce the perceived need for data localization and data sovereignty requirements, while at the same time protecting use privacy through due legal process.

Information about cross-border demands for data is relevant to our customers and stakeholders, and we will track and report these demands in our transparency report.

Surveillance by Governments

CONTEXT/TECHNOLOGY

Governments, intelligence services, and law enforcement agencies intercept communications on a regular basis to counter criminal and terrorist activities. Targeted communications interception and surveillance, subject to judicial review and oversight in a system of laws with due process and respect for human rights, can be used as an effective mechanism to anticipate and respond to evolving threats against national security and public safety. However, various governments have used mass surveillance, interception and data collection, and other approaches that are disproportionate to the risks, are not transparent, or are not subject to independent oversight.

HUMAN RIGHTS IMPACTS

Governments have increasingly threatened individuals' right to privacy through communications interception and/or the targeted surveillance of activists, human rights defenders, and journalists. Government surveillance, when unlawful and unjustified, undermines the right to privacy and other human rights (such as freedom of expression and freedom of association) that are enabled by privacy. Mass surveillance, often tied with censorship and social monitoring, can have a "chilling effect" on the exercise of essential freedoms and facilitate the repression of citizens.

CISCO RELEVANCE AND APPROACH

Cisco technologies and systems are used by government agencies to promote public safety, but the same technology can be used for surveillance that would violate individuals' privacy rights.

We maintain a policy of limiting the circumstances under which we will build electronic surveillance capabilities to lawful intercept requirements mandated by law. These circumstances are limited to those where electronic surveillance is required by applicable law in the jurisdictions where the technology is reasonably anticipated to be deployed; is consistent with Cisco's policies for privacy, security, customer data protection, and human rights; is requested by the customer deploying the equipment; and is publicly documented.

In the design of our products, we work to identify security issues and avoid vulnerabilities. We have also established a principled approach to government requests for data, with the intent of protecting our customers and users from unlawful, overbroad, or inappropriate government access to their data.

CISCO POINT OF VIEW

We believe that it is possible to have a society where safety, security, and private networking are not antithetical to national security.

We respect people's right to privacy and build encryption into our products that safeguards against arbitrary interference with that right.

We will only engineer, deploy, operate, or facilitate lawful intercept and electronic communications surveillance capabilities to the extent required by applicable law in the jurisdictions where the technology is reasonably anticipated to be deployed, and in accordance with the limited circumstances described above.

We will not include surveillance capabilities in a sale to customers in a country where we know those sales capabilities are illegal. We only include such capabilities to the extent required by applicable law.

We believe that law enforcement and national security agencies should go directly to our business and government customers to obtain information or data regarding those entities, their employees, and users. We do not provide information or access to users' data absent appropriate legal process.

We strive to protect our customers from unlawful government requests for data. Cisco is committed to publishing data regarding requests or demands for customer data that we receive from law enforcement and national security agencies around the world. We will review the scope and content of our transparency report over time as technology and our business evolves, and seek to increase stakeholder awareness of our approach.

We recognize that hacking by governments for reasons of information gathering and surveillance can occur, and believe that this practice should always be accompanied by robust substantive and procedural safeguards that provide human rights protections and respect the principles of necessity and proportionality. We encourage efforts by governments and multilateral institutions to establish a clear legal and policy framework for government hacking that minimizes privacy violations and limits the overall weakening of informational security. Any such government activities should only be undertaken with appropriate oversight and a clearly delineated disclosure process that allows vulnerabilities to be remedied in a timely fashion.

Internet of Things

CONTEXT/TECHNOLOGY

By 2030, 500 billion devices and objects will be connected to the internet. The rapid growth of this global IoT infrastructure has far-reaching technological and societal implications. These implications vary across the wide-range of IoT applications: connected cars, smart grid, e-health, wearables, smart home, and more. New products and services related to IoT will increase the security and privacy complexities of the environment through the physical devices themselves, the networks over which they communicate, and the back-end systems and data repositories.

HUMAN RIGHTS IMPACTS

IoT technology will do much to integrate existing and leading-edge technologies—enabling greater efficiencies and conveniences alongside new privacy and security risks:

- Surveillance: Internet-connected toys, cars, homes, and devices can be used by attackers to monitor the movement and activities of users. This surveillance may not only violate users' privacy, but could also chill free expression.
- Data privacy: IoT technology enables the creation, collection, storage, and processing of significant amounts of data, both personal and environmental. These data flows are often streaming continuously and can be stored or analyzed at various parts of the network. The personal data collected may not always be protected or anonymized sufficiently to ensure the privacy of the data subject. Additionally, users may not be aware of the types of data being collected by their internet-connected things or may not have sufficient control over the collection and flow of their personal data.
- Cybersecurity: Not all internet-connected things have the same level of security, and in fact, many of the everyday consumer products are potentially vulnerable to attacks that could disrupt normal use or create safety concerns. These devices often have little to no physical security, are sold at low price points, present user interfaces that are constrained or absent entirely, and fail to follow basic software best practices. Furthermore, some devices may not have upgradeability or software patching capability—this is particularly true for low-cost or basic devices. For example, internet-connected children's toys, household appliances, and wearable devices on the market today are vulnerable to being compromised as companies have not built in the level of privacy and security necessary for any networked device.

CISCO RELEVANCE AND APPROACH

Cisco has a significant role in the enablement of the Internet of Things. We connect millions of endpoints—cars, home security systems, point of sale devices, pacemakers, energy meters, etc.—across the IoT ecosystem. We serve IoT customers with products like IoT Networking, Control Center, IoT Management, Application Enablement, IOx and Fog Applications, Kinetic, and Extended Enterprise.

We don't make consumer products and sensors, but we are integrally tied to the IoT ecosystem and provide Cisco security to our customers. For example, we offer security architecture and services to customers through Cisco IoT Threat Defense Portfolio.

Cisco works with suppliers to deploy the latest IoT technology in manufacturing facilities to track, monitor, and improve the efficiency of our supply chain. When doing so we work with suppliers to respect the rights of our manufacturing workers and incorporate safeguards necessary to ensure that privacy, security, and safety rights are not infringed.

CISCO POINT OF VIEW

We believe that IoT technology has huge potential to enable innovation and create positive societal impacts. The connection of billions of devices enables the collection, routing, and analysis of massive amounts of data, leading to benefits like optimized business operations, reduced energy usage and greenhouse gas emissions, improved human health outcomes, and many more. However, the success of IoT technology requires manufacturers and services providers to follow best practice, as well as the generation and maintenance of trust in privacy and security standards.

We have set out a proposed Framework for Securing the Internet of Things.

We expect our customers to own and manage data in a manner that respects the human rights of the end user. This includes ensuring the end user has awareness of and control over the data they are sharing. We help and encourage our customers to follow best practices, such as rights-respecting terms of service, location privacy, a set date for data expiry, a purpose limitation for the data collected, and strict rules for data minimization.

We support a flexible framework to secure the IoT environment comprised of four components—authentication; authorization; network enforced policy; and secure analytics: visibility and control—which we implement within our own products and services and encourage amongst our customers.

We use our supply chain as testing grounds for how IoT can enhance productivity, efficiency, and human wellbeing. However, when doing so, we are attentive to potential human rights impacts that might arise from the use of IoT in a factory setting—such as impacts on privacy, non-discrimination, and labor rights—by raising these issues directly with our suppliers.

Big Data Analytics

CONTEXT/TECHNOLOGY

Big data[1] and associated technologies are quickly becoming an underlying component of how we engage with people and things each day. From social media and internet use to mobile devices and the internet of things (IOT), more and more data is being collected about our choices, preferences, and activities. With this growth in the amount and type of data available, new data techniques and tools have been developed to expand companies and governments' abilities to collect, store, and analyze data on a scale larger and faster than ever before.

The positive potential of big data is significant: greater customization of products and services; faster and improved health solutions and tracking of humanitarian needs or human trafficking risks. However, datasets and algorithms can have inherent flaws and are prone to error. The unintended consequences of big data can be especially harmful for vulnerable populations and can undermine individual and societal human rights.

HUMAN RIGHTS IMPACTS

Big data can be a source of insight and a driver of innovation and growth. At the same time, it can also be used, whether intentionally or unintentionally, in a manner that adversely affects individuals and societal groups.

At a high level, there are issues of ownership, accountability, and transparency of big data sets. To ensure the privacy of individuals' personal data, companies must be transparent about the data they collect, and the mechanisms used to process and analyze that data. This requires the company to have a full understanding of who is using big data within the company and for what purpose, and what the outcomes of the analysis are, whether intended or not.

At a functional level, how a company collects, processes, and analyzes data can put human rights at risk. It will be increasingly important to ensure algorithmic bias and discrimination risks are identified and mitigated at the outset. Other issues include insufficient encryption, potential breaches of privacy, and lack of anonymity.

CISCO RELEVANCE AND APPROACH

Cisco offers big data and analytics solutions through our Unified Computing System (UCS) integrated infrastructure and data applications. We do not sell, purchase, or monetize customers' data, and thus have a markedly different privacy risk profile than companies that do when it comes to issues of misusing data in violation of customer expectations.

[1] Cisco defines big data as the ability to capture, aggregate, and process an ever-increasing volume, velocity, and variety of data. The type of data being collected, stored, and processed is infinite in its variety and purpose, ranging from consumer spending and retail habits, to taste in music or books, to sensitive patient and healthcare information, to financial information.

We believe that our technology can be used for positive human rights impacts. For example, the Australian analytics firm Quantium developed a big data solution that runs on Cisco UCS infrastructure and uses our MapR Converged Data Platform. Using India's census data, government education data and other sources, Quantium looks for factors such as drought, poverty level, proximity to transportation stations, educational opportunities, population, and distance to police stations to identify the villages and towns that are most at risk of human trafficking.

CISCO POINT OF VIEW

We recognize that concepts like consent, ethics, and privacy may differ between countries and cultures. We will strive to develop a clear standard for how we interpret the application of these concepts to our products and engagement with customers, while being respectful of cultural differences.

We will continue to inform our customers of the types of personal data we process and the purpose of processing.

We will continue to build functionality into our products that allows customers to better control the collection and use of their data. Ultimately our customers should use those functions and inform end users about their capabilities and limitations in a manner that respects the human rights of the data subjects and data owners. This includes ensuring the end user has awareness of and control over the data they are sharing and how it will be used.

When governments and law enforcement agencies seek data in the course of an investigation, we believe this data should be obtained from the enterprise customer, rather than the third-party cloud service provider. As noted above, where customer data or other data about the customer’s use of Cisco technology is demanded directly from Cisco, we will publicly report on government and law enforcement requests as permitted by law.

We will strive to better understand the data we collect, store, and process internally (for human resources and supply chain purposes), and we will seek to use this data responsibly, with respect for human rights.

Artificial Intelligence

CONTEXT/TECHNOLOGY

Artificial intelligence (AI) and related technologies, such as machine learning and deep learning, are fundamentally changing the way Cisco and our customers engage with the world. AI has the vast potential to improve people’s quality of life, increase business efficiency and productivity, and augment society’s capacity to tackle global challenges. However, rapid advancements in AI technology require close attention to issues of safety, trustworthiness, transparency, fairness, ethics, and equity. These issues can manifest as risks to fundamental human rights, particularly when the consequences of such new technology can’t all be anticipated. The pace at which AI is developing, and the many unknown impacts—both positive and negative—on individuals and communities around the world necessitate business commitments to proactively respect human rights in the design, development, and use of AI.

HUMAN RIGHTS IMPACTS

New human rights risks and opportunities will arise as AI technologies develop. While not comprehensive, the human rights implications below illustrate the types of potential impacts companies, individuals, and governments will need to address.

- Non-discrimination (UDHR Article 7): Well-designed AI has immense opportunity to eliminate human bias from decision making. However, AI can also inadvertently disadvantage or harm an individual based on their race, sex, language, religion, or other personal characteristics. This risk typically emerges from biased data or algorithms within a machine learning system or process—examples of when AI could be used in a discriminatory manner include using AI for sentencing decisions in courts, providing access to credit, shortlisting job candidates, or identifying potential terrorists.
- Privacy (UDHR Article 12): The use of AI in surveillance infrastructure and law enforcement can infringe upon an individual’s right to privacy. Privacy enables the realization of other rights, and thus a violation of an individual’s privacy can lead to subsequent violations of their life, liberty, and security of person (Article 3), the right to freedom of opinion and expression (Article 19), and the right to freedom of peaceful assembly and association (Article 20), among others.
- Freedom of expression (UDHR Article 19): Well-designed AI can help companies address challenges such as hate speech, terrorist content, information security, or child exploitation imagery at scale. However, online content is increasingly reviewed

using AI technology, putting at risk an individual's right to freedom of opinion and expression—this risk is most likely to emerge when using AI to review social media content for terms of service compliance.

- Child rights (Convention on the Rights of the Child): Children's rights (unique from those of their parents and other adults) can be put at risk by the more widespread use of AI in voice recognition technology, smart personal assistants, smart toys, and educational systems. This technology can bring significant benefits to children's' growth and development, but safeguards for their privacy, moral well-being, and physical and mental health must be in place.
- Labor rights (UDHR Article 23 and ILO Core Conventions): While many jobs are made more efficient and effective through the integration of AI, there are other areas where workers, particularly low-skilled workers, are at risk of being replaced by AI. Without proper retraining and supportive workforce transitions, this mass displacement of workers by machines could push many into unemployment, under employment, or precarious work—significantly impacting their right to fair and decent work.

CISCO RELEVANCE AND APPROACH

AI is leveraging the vast amounts of data being collected by networked systems and devices in the Internet of Things. In addition, Cisco is using AI technology in our products and services to protect networks and assets, improve efficiency, and create more value for our customers.

For example, we recently launched Encrypted Traffic Analytics (ETA), an AI-driven solution using machine learning to analyze encrypted network traffic, and automatically identify and eliminate malware threats. This allows the information to remain encrypted and helps protect privacy and security simultaneously.

Additionally, we have recently acquired MindMeld and use the new technology to support Cisco WebEx Teams and other user interfaces. These interfaces are now more natural, intuitive, and intelligent, enabling our customers to be more productive.

Moreover, AI has the potential to deliver many positive societal benefits, and Cisco is supporting the development of AI solutions for today's global problems. For example, the Cisco Talos AI team entered the Fake News Challenge, a competition created to foster development of AI to detect fake news stories, and won first place.

Regarding AI and the future of work, we have teamed up with Oxford Economics to research the impact technology will have on the labor market as existing jobs are automated. This has helped us better understand the changing nature of work and identify where there are reskilling opportunities to maximize inclusion.

CISCO POINT OF VIEW

We believe that AI has enormous potential for society. Many applications of AI will have a highly positive impact on human rights, and we believe in developing AI technology that enables innovation and addresses major social challenges such as health care, education, and transportation.

However, AI will be used for bad as well as good, and certain actors will either exploit the technology for abusive purposes, or not deploy effective protections against adverse human rights impacts. We believe action can be taken to minimize these impacts. Cisco has active projects to identify bad actors and negative uses of ML/AI.

We will raise awareness among relevant Cisco technical employees and engineers on human rights issues, for example by identifying higher risk AI use cases and scenarios. We will support academic programs that enhance ethics and human rights training in the technical and engineering professions.

We support an increased dialogue and collaboration between professions—technical experts and engineers, human rights and ethics experts, lawyers, researchers, law makers, and law enforcement—to improve our collective understanding of the societal and human rights impact of AI and machine learning. We believe that Cisco's role is to bring high levels of technology, engineering and product development knowledge, insight, and expertise to this dialogue.

We have a responsibility to ensure that vulnerable workers in our supply chain are not facing significant negative impacts of AI and automation. We support our suppliers in reskilling workers to be redeployed when necessary and believe AI can bridge skill gaps between Cisco and its supply chain.

Engagement, Product Design, and Sales

Across all these disruptive technologies, Cisco’s approach includes a responsible and proactive approach to product design, sales, engagement, and collaboration.

On product design, we are committed to taking a “human rights by design” approach to disruptive technologies such as AI and IoT, assessing the potential human rights risks and opportunities of new products and reviewing the long-term impacts of existing products. To support this goal, we will raise awareness among relevant Cisco technical employees and engineers of best practices and guidance on how to integrate human rights into the product design and development process.

On sales, our Global Export Trade team ensures compliance with controls under the U.S. Export Administration Regulations and Wassenaar Arrangement by creating US and country-specific export policies and guidelines to ensure Cisco's conformance with its obligations. All transactions undergo a compliance check to ensure that none of the parties to a sale are listed on any applicable sanctioned or denied entity list.

However, not every sale that is legal should be made, and we recognize that developments in technology will increase the need for consideration of ethical and human rights factors in business decision making. We will draw upon the expertise of our Global Export Trade team, Security & Trust Organization, Ethics Office, Government Affairs team, Corporate Affairs team, and other relevant groups to further develop our ethical and human rights framework, complement our existing decision-making processes, and provide support for sales teams and country managers faced with increasingly complex dilemmas.

On engagement and collaboration, Cisco is an active participant in a wide range of standards-setting and industry organizations that are helping shape the future norms, standards, and approaches of relevance for technology and human rights. These include the Alliance for Open Media, Alliance for Telecommunications Industry Solutions, Blockchain IoT Protocol Initiative, Broadband Internet Technical Advisory Group, Center for Information Policy Leadership, Cloud Security Alliance, International Association of Privacy Professionals, Internet Engineering Task Force, Internet Governance Forum, Institute of Electrical and Electronics Engineers Standards Association, ITU Telecommunication Standardization Sector, Metro Ethernet Forum, LoRa Alliance, National Cyber Security Alliance, Payment Card Industry Board of Advisors, Responsible Business Alliance, TechNet, Trusted IoT Alliance, and the World Wide Web Consortium.

Conclusion

We believe it is our responsibility to continually improve how we implement our human rights principles. This commitment to continuous improvement is especially relevant in the context of disruptive technologies and trends that develop in uncertain ways and will transform the business and human rights landscape. We are also committed to understanding how our human rights impacts, risks, and opportunities will evolve over time, and to addressing them in a collaborative, transparent, and solutions-oriented manner. To fulfill this commitment, we will continue to engage with our stakeholders proactively, communicate progress in our annual Corporate Social Responsibility report and website, and review and update these position statements as needed over time.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.