Global Guiding Principles for Trust, Technology and Government Access in the Digital Age

Recognizing that protecting the fundamental values of security, privacy, freedom of expression, and openness are essential to earning citizens' trust in technology in the global marketplace; and

Recognizing governments have legitimate needs to seek access to technology or data of commercial entities, including for law enforcement, intelligence, counterterrorism, or national security purposes;

The principles below are intended to guide governments in developing policies to enable government access to technology, and to express the tech sector's commitment to working with governments to develop such policies, consistent with advancing the fundamental values of security, privacy, and trust.

Value and Protect Citizen and Customer Trust

Prioritize Security and Privacy. *Privacy, security, and personal safety are fundamental human values.* As such, the tech sector develops technology that maximizes these precepts. Issues at the intersection of privacy and security are too often portrayed in an absolutist or a binary fashion, but while distinct the two are inextricably linked in the digital world: there is no security without privacy and there is no privacy without security. Both are critical for personal safety. We believe government policies should reflect this reality.

Oppose Weakening the Security of Technology Products and Services. *Robust cybersecurity and data protection are essential to trust in technology products, services, and systems, and robust encryption is fundamental to building such trustworthy and reliable technology products, services, and systems.* The tech sector does not deliberately undermine the security of our products, services, systems, or data, and we maintain the confidentiality of source code and design information to protect the security of our customers, products, and services. We reject imposing legal mandates on technology providers to decrypt information when they do not retain physical possession of encryption keys or other technical means to decrypt such information, as well as other requests to circumvent or compromise the security features in those products or services, including requests to escrow encryption keys or source code.

Respect Freedom of Expression and Privacy as Essential Values. *The tech sector strongly supports the right of citizens to expression, to exchange data across borders, and the right to privacy as foundational underpinnings of human dignity.* We acknowledge a responsibility to respect and protect the freedom of expression and the privacy of our customers. The tech sector is also committed to working with governments to collectively help counter online terrorist propaganda. We encourage all governments to respect this position, which is both consistent with Article 19 of the Universal Declaration of Human Rights and with local laws in many geographies.

Embrace Openness and Global Markets to Enable Security Innovation and Interoperability

Support Policies and Practices to Enable Trust in Technology Products and Services. *Advancing the trustworthiness and security of technology and services is indispensable to protect citizens' data from hackers, cyber thieves, and those who would inflict physical harm.* The tech sector incorporates strong security features into our products and services to advance trust, including using published algorithms as our default cryptography approach as they have the greatest trust among global stakeholders, and limiting access to encryption keys. We encourage governments to fully leverage strong, globally accepted and deployed cryptography and other security standards that enable trust and interoperability.

Nurture Global, Market-Driven Product Development Approaches and Testing Protocols for Security. *Trust, global technology interoperability, and open data flows are essential for technology development and*

innovation, and thus fundamental to the growth, security, and stability of global commerce and critical infrastructure. The tech sector uses and continually seeks to improve global, voluntary, consensus-based standards and best practices in design, development, manufacturing, and testing processes to build security and privacy into our products and services, including performing security validation before shipping a product or offering a service. To preserve the interoperability and trust necessary for economic growth and stability, governments should avoid policies that threaten the borderless Internet, such as data localization requirements, the extraterritorial application of laws, market access restrictions, and design requirements for technology products and services, including requirements related to encryption or communications access.

Commit to Openness and Global Norms in Recognition of the Global Technology Marketplace. *Technology goods and services are developed, marketed, and sold globally.* The tech sector develops products and services for people around the world and is committed to trust, integrity, and resiliency in those products and services, regardless of the markets in which we operate. Together with our suppliers and customers globally, we work to advance the reliability, resiliency, security, and integrity of our supply chains, support policy processes that are open, transparent, and consultative, and oppose mandates that establish regulatory preferences for specific types of security technologies. Governments should recognize that country-specific restrictions on the availability of certain technologies are unlikely to significantly impact the availability of such products, particularly to "bad actors" such as criminals, hackers, or terrorists.

Employ Responsible and Equitable Security Vulnerability Disclosure and Remediation Practices. *Sensible vulnerability disclosure and remediation practices by all parties are essential to the security of the digital ecosystem.* The tech sector takes timely action to analyze and mitigate the risk of discovered vulnerabilities and follows responsible disclosure practices to notify our suppliers, resellers, customers, and others as appropriate. We urge governments to likewise adopt transparent policies to disclose vulnerabilities to technology vendors in a timely fashion to enable them to better protect against cybersecurity attacks and that encourage responsible disclosure of vulnerabilities by security researchers to technology vendors.

Collaborate and Build Capacity to Address Government Access Challenges

Leverage Multi-Stakeholder Partnerships to Drive Durable Solutions. *Addressing the complex questions at the intersection of security, technology, privacy, and economic growth requires collaboration between a diverse set of stakeholders, including law enforcement, tech and other business sectors, academia, and privacy and civil liberties advocates.* The tech sector is committed to constructively engaging in efforts to transparently convene representatives of these groups in task forces or roundtables to inform policymaking and encourage public participation by publishing proposed policies and regulations for public comment. We welcome governments everywhere as partners in this effort.

Prioritize Mutual Legal Assistance Reform and Cooperation. *Governments investigating criminal activities increasingly require extraterritorial access to electronic evidence.* To increase public safety and security and make investigations and prosecutions more efficient, governments should expand investment in cross-border data request mechanisms for law enforcement and counterterrorism purposes, including making Mutual Legal Assistance Treaties (MLATs) more effective tools for cross-border investigations, and leverage existing multilateral agreements, such as the Budapest Convention on Cybercrime. We support a call to action to all governments to prioritize global law enforcement coordination to better address these issues.

Increase Governments' Technical Expertise. *Protecting and defending against national security and terrorist threats and upholding and enforcing criminal laws are fundamental missions of governments around the world.* Technology can be a central tool in furthering these missions. Consistent with the tech sector's unwavering commitment to security and privacy, we are prepared to work transparently as a part of collaborative efforts with governments to improve the technical competencies of their workforce, to build capacity to understand the rapidly evolving nature of technology, to help prioritize resources, and to leverage technological innovation to assist in conducting lawful investigations.