Microsoft

SIX PRINCIPLES FOR INTERNATIONAL AGREEMENTS GOVERNING LAW-ENFORCEMENT ACCESS TO DATA

1. THE UNIVERSAL RIGHT TO NOTICE: Absent narrow circumstances, users have a right to know when the government accesses their data, and cloud providers must have a right to tell them.

Individuals and organizations have a right to know when governments access their digital information. In certain cases, alerting the target of a law enforcement demand may imperil an ongoing investigation or result in further danger to public safety. While secrecy orders are appropriate in those limited circumstances, international agreements must make clear that secrecy should always be the exception, not the rule.

When secrecy is required, investigators should be required to (1) make their case for secrecy to an independent authority, such as a judge; and (2) present case-specific facts to justify both why the government itself should not be obligated to notify the target and why the government must limit the cloud provider's right to notify its customers of the request. Any nondisclosure order imposed on a cloud provider must be narrowly limited in duration and scope, and must not constrain the provider's right to speak any more than is necessary to serve law enforcement's demonstrated need for secrecy. Cloud providers must also be permitted to challenge these orders to ensure that government nondisclosure orders satisfy these requirements.

In the United States, Microsoft has fought hard to secure these rights and protections. Three times we filed lawsuits against the U.S. government to increase transparency, and all three successfully prompted significant new protections for our customers. Governments seeking to send law enforcement demands directly to foreign cloud providers through an international agreement should be held to similarly high standards.

2. PRIOR INDEPENDENT JUDICIAL AUTHORIZATION AND REQUIRED MINIMUM SHOWING: Law enforcement demands for content and other sensitive user data must be reviewed and approved by an independent judicial authority *prior to* enforcement of the order, and only after a meaningful minimum legal and factual showing.

Independent judicial authorization of law enforcement demands for content and other sensitive electronic data is essential to any legal framework that seeks to promote the rule of law and ensure public confidence in government. Though governments around the world will determine their own appropriate legal standards and procedures, there must be a universal requirement that all demands for content and other sensitive digital evidence be reviewed and approved by an independent judicial authority based on a required minimum showing prior to law enforcement seeking disclosure of data. Prior review and approval by an independent judicial authority is the only globally accepted structural mechanism that meaningfully protects privacy and fundamental rights. It guards against overbroad and unlawful demands for customer data. It also serves to advance the overall legitimacy of the law enforcement investigation itself.

The standards that govern prior, independent judicial authorization should also be rigorous, providing adequate protection for personal privacy and against government overreach or abuse. For example,

requests should be targeted at a specific account, identifier or device. In addition, requests should only be approved when they are supported by specific evidence that demonstrates criminal conduct and that the data demanded is needed in connection with an investigation of a serious criminal offense.

Existing law in the United States requires prior judicial authorization of orders seeking all categories of digital evidence held by cloud providers, except for demands for a specific, limited set of basic subscriber information (which may be requested by law enforcement via subpoena). Law enforcement in the United States must obtain a warrant – issued by a neutral magistrate based on a specific factual finding of probable cause of a crime – to obtain content or location information (over an extended period), and must obtain a different form of court order to obtain transactional logs and other types of metadata**.** Any government seeking to send law enforcement demands directly to a foreign cloud provider must be required to adopt similar forms of prior independent judicial authorization based on a meaningful minimum legal and factual showing.

3. SPECIFIC AND COMPLETE LEGAL PROCESS AND CLEAR GROUNDS TO CHALLENGE: Cloud 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.

Cloud providers act as a critical check to ensure that governments' use of their investigative powers strictly adhere to the rule of law. When law enforcement seeks access to customer data, cloud providers' thorough review of law enforcement demands serve to ensure that governments are respecting the rights of internet users around the world. These users have an expectation that cloud providers will receive sufficiently detailed legal process from governments that will allow them to identify and challenge inappropriate demands in court prior to disclosure of their sensitive data.

Therefore**,** governments seeking to send law enforcement demands directly to foreign cloud providers through an international agreement must, at the very least, be required to establish on the face of the demand (1) that appropriate prior independent judicial review and approval was obtained; (2) that the investigation involves a specifically identified serious crime as defined by the terms of the corresponding international agreement; and (3) that the demand is not in furtherance of an investigation that infringes on internationally recognized fundamental human rights.

Specific and complete legal process is only meaningful if cloud providers can avail themselves of clear procedural and substantive rights to challenge demands that are overbroad, abusive, violate the terms of an international agreement or are otherwise unlawful. Accordingly, governments seeking international agreements must also provide foreign cloud providers with clear mechanisms in their domestic law or under the international agreement to challenge unlawful demands for data.

4. MECHANISMS TO RESOLVE AND RAISE CONFLICTS WITH THIRD-COUNTRY LAWS: International agreements must avoid conflicts of law with third countries and include mechanisms to resolve conflicts in case they do arise.

Government-to-government dialogue and international agreements are the only legitimate mechanisms to facilitate cross-border demands for electronic evidence in a manner that respects international borders and sovereignty. An international agreement between two countries, however, may not resolve all conflicts that might arise with a specific law enforcement demand, particularly when the demand implicates a third country's citizens or laws. Consequently, international

agreements must contain mechanisms to resolve or raise potential conflicts directly with third-party countries when such conflicts arise.

5. MODERNIZING RULES FOR SEEKING ENTERPRISE DATA: Enterprises have a right to control their data and should receive law enforcement requests directly.

Public and private organizations – and even governments themselves – are increasingly moving their digital information to the cloud. Transition to cloud-based infrastructure, however, should not change the basic principle that these enterprises have a right to control their data and receive investigatory demands directly from law enforcement.

Absent extraordinary circumstances, seeking data directly from enterprises will not compromise a law enforcement investigation or result in a danger to public safety. This is especially true when the legal demand implicates large organizations, which likely have an interest in cooperating with law enforcement.

Recognizing that law enforcement practices must evolve with changing technology, the U.S. Department of Justice and the European Commission have both taken strong stands that investigators should seek data directly from the enterprise, rather than cloud-storage providers, if doing so will not compromise the investigation. Governments seeking to send law enforcement demands directly to foreign cloud providers through an international agreement should similarly modernize and memorialize investigatory rules to guard against improper law enforcement demands for enterprise data, particularly when such requests are better and more efficiently directed at enterprise companies themselves.

6. TRANSPARENCY: The public has a right to know how and when governments seek access to digital evidence, and about the protections that apply to their data.

Transparency in the negotiation and implementation of international agreements is essential to maintaining public trust in government and technology. Reflecting democratic traditions and principles, governments must be transparent when negotiating agreements that govern the standards for cross-border law enforcement requests for digital evidence and the protections that apply to their respective residents. At minimum, governments must be required to publish the text of the proposed agreement prior to its adoption to allow for meaningful public input. All agreements must also ensure that cloud providers have the right to publish regular and appropriate transparency reports that document the number of demands they are receiving, the number of customer accounts that are affected and the government issuing these orders. At Microsoft, we believe it is our responsibility to provide the public with this data, and we commit to doing so.

In the United States, Microsoft and a coalition of other companies sued the U.S. Government to share more information with the public about the national security orders we receive, insisting that it was our right to do so under the First Amendment of the Constitution. Our right and our obligation to be transparent with our users must not be eroded by international agreements that fail to maintain the same level of transparency for government demands for digital evidence.