



Security and Privacy in Lawful Government Access

Government access to private and commercially sensitive data remains a contentious issue in countries around the world. On one hand, governments have a set of law enforcement and national security responsibilities that may involve their seeking information on individuals and entities of concern. As the cloud aggregates large amounts of personal and confidential or proprietary information, it has become a target for government access requests in support of law enforcement activities, in particular.¹ Yet, broad authorities to access this information could be abused for political and other purposes. Moreover, the excessive use of such authorities risks undermining customers' confidence in the cloud as a global operating environment. As governments seek access to cloud-hosted data, they must weigh the security benefits of their actions against the potential privacy costs.

Key Considerations

- ***Differing definitions of “access.”*** Around the world, domestic laws² provide different and potentially conflicting definitions of lawful access, including on its degree, duration, process, and the roles of cloud providers and their customers in facilitating that access.³ As a result, there is no consistent and fair balance between privacy rights and law enforcement needs across countries. Moreover, the issue is politically charged within and among countries, leading that balance to fluctuate as stakeholder interests change.
- ***Threat of access undermines trust.*** The threat of unfettered government access to cloud-hosted data may undermine customers' and other governments' trust in those services, even if the threat does not materialize.⁴
- ***Recipients of access requests.*** It is more efficient for government agencies to request data on a range of targets from a single cloud provider than to send individual requests to many enterprise customers for the same data. The potential for efficient access to vast amounts of sensitive data generates anxiety about its implications for civil liberties and the potential for abuse.⁵
- ***Barriers to disclosing access requests and seeking redress.*** Providers are not presently required to inform customers about government requests for their data (unless stipulated in a contract), but sometimes voluntarily disclose this information privately to enterprise customers⁶ and in anonymized transparency reports.⁷ Governments may use gag or secrecy orders on providers to prevent disclosure of access requests, preventing customers from learning of government attempts to access private data.⁸ Additionally, in less democratic regimes, providers (and their customers) might lack an independent and transparent domestic process for challenging government access requests.

- **Access can create security vulnerabilities.** Some forms of sustained government access can create security vulnerabilities,⁹ for example, if achieved by undermining privacy- and security-enhancing mechanisms (for example, via the creation of back doors or other methods of undermining encryption).
- **Balancing the need to remain a competitive market for providers.** In crafting lawful access policies, governments are forced to balance their security responsibilities against the risks that unfettered government access could deter cloud providers from offering services to their populations. This could limit the population’s choices to only those providers willing to comply with the government’s policy or, potentially deny them the cloud’s economic and social benefits altogether.

Stakeholder Perspectives

Government

- Seek timely access to cloud-hosted data and services, potentially both at rest and in transit.
- Interested in restricting foreign governments’ access to cloud services and cloud-hosted data.
- Express varying degrees of interest in ensuring that arrangements to grant them access to the cloud do not excessively compromise individual privacy and commercial confidentiality.

Cloud Providers

- Eager to minimize the scope, duration, and rationales for government access to cloud systems and data.
- Aim to comply in a timely fashion with legal requests from the government.
- Seek to retain ability to challenge the legality of government requests.
- Wish to maintain customer trust by demonstrating a cautious approach to fulfilling government access requests and offering transparency into

Customers

- Wish to be informed and have the ability to challenge government access requests or other demands pertaining to their cloud services.
- Wish to retain the ability to move and keep data where they want it, securely and privately.
- Wish to use cloud services that neither undermine nor excessively impede government investigative and law enforcement functions.¹⁰

Others

- N/A

how such requests are fulfilled.

- Want to navigate the different (and potentially irreconcilable) legal obligations that may exist across their domestic and foreign operations.

Tensions with Other Cloud Governance Issues

- **Privacy Protections:** Recognizing the cross-border nature of cloud-hosted data, national policies on what constitutes lawful government access to cloud services and data may grant governments access to data physically located outside of their jurisdictions, potentially implicating the privacy of customers abroad.
- **Restricting Exports of Cloud Services to Human Rights Violators:** Although governments often seek access for themselves, they may seek to deny such access to other governments whom they suspect will exploit cloud services and cloud-hosted data to encroach on human and civil rights. As a result, some governments may restrict exports to nations with expansive government access authorities.
- **Localization and Routing Requirements:** Permissive government access authorities may be used as justification for others to impose data localization requirements and routing restrictions, impairing the free flow of data across jurisdictions.

Potential Ways Ahead

Government	Providers	Customers	Others
<ul style="list-style-type: none">• Wherever possible, direct access requests to customers rather than to cloud providers.• Allow cloud providers to notify enterprise customers in	<ul style="list-style-type: none">• Inform enterprise customers of government access requests in every circumstance permitted by law.¹³• Publish, on a regular basis, transparency reports detailing aggregate statistics	<ul style="list-style-type: none">• <i>Enterprise Customers:</i> Publish, on a regular basis, transparency reports detailing aggregate statistics on government access requests (including requests received from	<ul style="list-style-type: none">• N/A

advance of government access to their data, other than in exceptional circumstances, for example by limiting the use of secrecy orders.¹¹

- Mandate scoping, oversight, and transparency on government access requests (including requests received from foreign governments).
- Work with foreign governments to establish international agreements and mechanisms to resolve conflicts of laws and to ensure that foreign government access to data does not impinge on the privacy of citizens, national security, or defense.¹²

on government access requests (including requests received from foreign governments).¹⁴ (Shared with Enterprise Customers.)

- Develop industry standards for challenging and, where appropriate, rejecting certain overbroad government access requests (for example, requesting unfettered access, encryption keys, and ability to break encryption). (Shared with Enterprise Customers.)
- Dissuade government access requests that do not meet agreed-upon criteria (such as requesting unfettered access, encryption keys, and ability to break encryption) and challenge these requests through legal actions and public relations.

foreign governments).¹⁵ (Shared with Cloud Providers.)

- *Enterprise Customers:* Develop industry standards for challenging certain overbroad government access requests (for example, requesting unfettered access, encryption keys, and ability to break encryption). (Shared with Cloud Providers.)

Recent Examples and Additional Resources

- “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,” *The New York Times*, May 17, 2021, <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html>
- “The CLOUD Act is an important step forward, but now more steps need to follow,” Microsoft (Blog), April 3, 2018, <https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/>
- “The need for a Digital Geneva Convention,” Microsoft (Blog), February 14, 2017, <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.
- “The Cybersecurity 202: Paul Manafort’s case may undermine the FBI’s encryption argument,” *The Washington Post*, June 6, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/06/the-cybersecurity-202-paul-manafort-s-case-may-undermine-the-fbi-s-encryption-argument/5b16ae5e1b326b08e8839150/?no_nav=true.
- “Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy,” OECD, December 2020, <https://www.oecd.org/sti/ieconomy/trusted-government-access-personal-data-private-sector.htm>.
- “WhatsApp adds end-to-end encryption to chat backups, locking up data in the cloud,” Cyber Scoop, September 10, 2021, <https://www.cyberscoop.com/whatsapp-encryption-backup-chats/>.

Notes

¹ See: Microsoft, “Law Enforcement Requests Report.” Microsoft, 2021, <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.

² See: Ju (Lindsay) Zhu, “China Passes New Data Privacy and Security Laws,” *The National Law Review*, August 23, 2021, <https://www.natlawreview.com/article/china-passes-new-data-privacy-and-security-laws>.

³ In the case of enterprise cloud deployments, cloud providers may re-direct access requests to the owners of the data, the enterprise customers themselves.

⁴ A similar effect has been observed in the past. For example, Edward Snowden’s revealing of U.S. National Security Agency surveillance programs damaged customer trust in U.S. technology companies and their products, both domestically and globally. See: The New York Times, “Revelations of N.S.A. Spying Cost U.S. Tech Companies.” *The New York Times*, March 21, 2014, <https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>.

⁵ Mechanisms for data storage and backup in the cloud further enhance the appeal of gaining access to the cloud as a repository of data, bypassing restrictions and difficulties of accessing data elsewhere. Trusted Cloud Principles, “Principles.” Trusted Cloud Principles, 2021, <https://trustedcloudprinciples.com/principles/>.

⁶ See: Microsoft, “About our practices and your data: Q: Does Microsoft notify its enterprise customers when law enforcement or another governmental entity requests their data?” Microsoft (Blog), n.d., <https://blogs.microsoft.com/datalaw/our-practices/#does-microsoft-notify-enterprise-customers>.

⁷ See: Microsoft, “Law Enforcement Requests Report,” Microsoft, 2021, <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.

⁸ Even when gag orders are not in place, providers may still fail to disclose government access requests to their customers.

⁹ See: “Open Letter to GCHQ,” Coalition of civil society organizations, technology companies, trade associations, and security and policy experts, May 22, 2019, [https://newamericadotorg.s3.amazonaws.com/documents/Coalition Letter to GCHQ on Ghost Proposal - May 22 2019.pdf](https://newamericadotorg.s3.amazonaws.com/documents/Coalition+Letter+to+GCHQ+on+Ghost+Proposal+-+May+22+2019.pdf).


¹⁰ Customers in any given jurisdiction are also citizens/residents and thus have an interest in refraining from utilizing cloud services/providers which undermine or excessively impede government access, to the point where traditional security threats and other undesirable law enforcement outcomes (such as the proliferation of terrorism-related material or CSAM) abounds.

¹¹ See: Jay Greene and Drew Harwell, “When the FBI seizes your messages from Big Tech, you may not know it for years,” *The Washington Post*, September 25, 2021, <https://www.washingtonpost.com/technology/2021/09/25/tech-subpoena-secrecy-fight/>.

¹² See: U.S. Department of Justice, “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,” U.S. Department of Justice, April 2019, <https://www.justice.gov/opa/press-release/file/1153446/download>.

¹³ See: Trusted Cloud Principles, “Principles,” Trusted Cloud Principles, 2021, <https://trustedcloudprinciples.com/principles/>.

¹⁴ Many cloud providers already produce information request reports on a voluntary basis, as part of their corporate social responsibility commitments. See: IBM, “IBM 1H 2021 Law Enforcement Requests Transparency Report,” IBM, 2021, <https://www.ibm.com/downloads/cas/DAGAKDJG> and Microsoft, “Law Enforcement Requests Report,” Microsoft, 2021, <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.



¹⁵ Many enterprise customers already produce information request reports on a voluntary basis, as part of their corporate social responsibility commitments. See: Twitter, “Information Requests,” Twitter Transparency Center, 2021, <https://transparency.twitter.com/en/reports/information-requests.html#2020-jul-dec>.