Privacy Protections

As the cloud centralizes large amounts of sensitive information, potential threats to the cloud raise data-privacy-related concerns. Privacy violations of cloud-hosted data can occur in multiple ways, including through security breaches that reveal data to unauthorized parties, the interception of cloud-hosted data in transit, and inadequate access management that allows unauthorized parties to obtain sensitive information.

Key Considerations

- ***Privacy rules vary internationally.*** Data privacy protections vary across countries and regions, and sometimes within countries, greatly complicating efforts to operate global cloud services and efficiently move data between jurisdictions.
- ***Disagreement over cryptographic key management.*** Cloud providers and customers may disagree over which party should be responsible for managing the cryptographic keys used to protect the privacy of cloud-hosted data and enable identity and access management. Many customers want greater control over their encrypted cloud-hosted data and wish to manage these keys themselves, but some cloud providers argue that customer data is more secure if providers manage the keys.[1] Complicating this debate are regulations that require government contractors and major customers in critical sectors to manage their own keys.[2]
- ***Operational costs of increased controls over sensitive data.*** Efforts to bolster customers' rights to control how their data in consumer cloud deployments is handled by cloud providers (for example, the location of storage, routing paths, and so on) may inhibit those providers from optimizing their services or achieving competitive advantage.

Stakeholder Perspectives

Government

- Wish to protect citizens' and other sensitive data from access by unauthorized actors, in some cases through rigid data localization requirements,

Providers

- Support improved rules and regulations, at both the national and international levels, that protect cloud customers' ownership of data as well as its

Customers

- Seek to secure robust protections against unauthorized access and invasion of privacy.
- Wish to be informed of and

Others

- *Human and civil rights advocacy groups:* Advocate for protecting and limiting the dissemination and use of customers'

national privacy laws, and so on.
    - May seek to establish the necessary legal, regulatory, and punitive frameworks thereof.
    - Seek the ability to access user data for law enforcement and national security purposes, such as surveillance or criminal investigations. Some also seek access for political and other purposes.

privacy and security.[3]
- Prioritize avoiding or limiting liability for privacy violations—as well as reputational damage and customer trust—as a result of access or use of sensitive customer information by unauthorized actors.
- Seek clarity on required safeguards or security measures to avoid liability.
- Wish to maintain user trust by protecting customers' identity and vital information.

compensated for privacy violations.
- Want to maintain discretion over how their sensitive information is collected, analyzed, and used.
- *Consumer customers*: Seek to hold cloud providers liable for data breaches and other security compromises.

sensitive information.

Tensions with Other Cloud Governance Issues

- ***Localization and Routing Requirements:*** Restricting access to data may negatively impact cross-border intelligence and information sharing arrangements.
- ***Security and Privacy in Lawful Government Access*** and ***Government Intervention in Extremis***: Government and law enforcement access may infringe on the privacy of cloud customers.
- ***Incident Handling Procedures***: Reporting requirements for breaches that implicate the privacy of cloud customers' sensitive information differ across jurisdictions.

Potential Ways Ahead

Government

- Require greater transparency in cloud computing contracts between customers and providers, particularly around responsibility for data privacy, liability for breaches, obligations for reporting and remedial action.
- Require increased transparency by providers and their customers on the collection, usage, storage, deletion, and other actions of specific types of data on a sector-by-sector basis.
- Provide model language on how to clearly allocate responsibilities and rights of parties with respect to data privacy.
- Define the ways in which impacted individuals may seek compensation for damages.
- Work with foreign governments to establish

Providers

- Set technical guardrails that discourage intrusions and continuously monitor/audit these protections for effectiveness.
- Create internal or engage external entities to investigate suspected breaches of user privacy.
- Provide robust technical mechanisms that allow customers to govern the collection and handling of their personal information.
- Clearly communicate to customers data collection, analysis, storage, and dissemination practices and policies; this can be in the form of easily accessible and digestible "principles."[4]
- Provide clear language on the allocation of responsibility

Customers

- Adopt basic measures that prevent/discourage cyber intrusions (for example, frequently changing passwords, two-factor authentication limiting what information is made public or shared with providers, and so on).
- *Enterprise customers:* Work with cloud service providers to ensure user identity and information are protected.
- *Enterprise customers:* Provide clear language on the allocation of responsibility between providers and customers for data privacy. (Shared with cloud providers.)

Others

- *Civil rights and other nongovernmental public interest groups:* Consult relevant parties (for example, privacy professionals and consumer groups) to craft policies that ensure user privacy and vital information is protected. Then, provide government or corporations with these recommendations.
- *Civil rights and other nongovernmental public interest groups:* Provide victims of privacy intrusion with legal counsel, represent them in cases of legal dispute.

international agreements and mechanisms to resolve conflicts of laws, in order to ensure the privacy of citizens' data as it moves across jurisdictions.
- Set guardrails for the degree of access governments may exercise in the event of government intervention.

between providers and customers for data privacy. (Shared with customers.)
- Ensure employees are well versed in corporate privacy principles and the pertinent laws and regulations.[5]

Recent Examples

- "Everything you need to know about the Microsoft Exchange Server hack," ZDNet, April 19, 2021.

Notes

[1] Brad Smith, "Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attach on SolarWinds (speech, Senate Select Committee on Intelligence, Open Hearing on the SolarWinds Hack, Washington, DC, February 23, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/os-bsmith-022321.pdf.

[2] Anton Chuvakin and Honna Segel, "Lost in translation: encryption, key management, and real security," Google Cloud (blog), September 11, 2020, https://cloud.google.com/blog/products/identity-security/how-encryption-and-key-management-enable-real-security.

[3] "Trusted Cloud Principles," Trusted Cloud Principles, n.d., https://trustedcloudprinciples.com/principles/.

[4] For example, "Data Security and Privacy Principles for IBM Cloud Services": IBM, "Data and Security Privacy Principles for IBM Cloud Services," IBM, n.d., https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW2/$file/Z126-7745-WW-2_05-2017_en_US.pdf.

[5] This may already be reflected in existing training and regulatory compliance activities.