



Restricting Exports of Cloud Services to Human Rights Violators

This issue concerns governments compelling CSPs—or CSPs voluntarily choosing—to deny or restrict the provision of cloud services to countries and organizations that violate human rights.

Key Considerations

- ***Uncertainty regarding role of cloud services in human rights violations.*** The international community does not have a clear way to assess how cloud technologies are or could be involved in facilitating human rights abuses by enterprise customers (for example, repressive governments), and it also does not have a clear understanding of how to mitigate such violations. Governments are likely to face serious resistance from providers when trying to impose human rights–based restrictions on the export of cloud services.
- ***Ineffective unilateral export controls.*** The lack of broad consensus on employing export controls for human rights purposes leads some governments to impose unilateral and potentially less-effective controls.¹
- ***Negative effects on local communities.*** Consumers living in countries that do not respect human rights may nevertheless want access to cloud-based services for reasons both related and unrelated to human rights. For example, they may want cloud-based services for commerce, social communications, and political organization. Restricting the sale of cloud services may have negative effects on cloud adoption, innovation, economic growth, and the prosperity of those communities.
- ***Less-scrupulous alternatives may become more attractive.*** Export controls might encourage human rights-violating regimes to seek cloud services from other suppliers. Alternative suppliers may maintain weaker access-management policies and practices, be less supportive of inclusive and equitable access to cloud services, and may be regulated by governments who may be less concerned with their companies’ culpability for human rights violations.
- ***Forced technology transfer may motivate export controls.*** Foreign governments may condition the ability to offer cloud services in their country on increased access to proprietary software and data, which providers often do not wish to turn over.

Stakeholder Perspectives

Government

- Do not wish to be seen facilitating the export of cloud services to known human rights violators. (Similar to cloud providers' perspective.)
- Seek to avoid becoming targets of foreign export restrictions that may hinder domestic cloud adoption.
- Want to balance export restrictions against the need to promote exports and ensure revenues for domestic companies.

Providers


- Wish to limit external influence over their choice of customers.
- Do not want to be held liable for the actions or activities of cloud customers.
- Seek to avoid reputational damage for being associated with or doing business with countries and organizations that violate human rights. (Similar to governments' perspective.)
- Lobby for distinctions between cloud services that directly abet human rights violations and general-use cloud services that are less directly implicated in such violations.
- Argue they are better positioned to influence the human rights practices of major customers (including governments) if

Customers

- Support or oppose export restrictions to human rights–violating entities depending on their personal political views.

Others

- *Human and civil rights advocacy groups*: Want to ensure that governments and providers refrain from doing business with countries and organizations that are known to violate human rights.



they are not
prohibited from
doing business with
them.

Tensions with Other Cloud Governance Issues

- **Equitable Cloud Access:** Restricting the export of cloud services may directly deprive sanctioned populations the opportunity to realize rights that are increasingly dependent on cloud access, such as education and expression.

Recent Examples

- Ellen Nakashima, “Biden administration slaps export controls on Chinese firms for aiding PLA weapons development,” *The Washington Post*, April 8, 2021, https://www.washingtonpost.com/national-security/biden-administration-slaps-export-controls-on-chinese-firms-for-aiding-pla-weapons-development/2021/04/07/0c45bf0a-97f6-11eb-b28d-bfa7bb5cb2a5_story.html.
- Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, “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>.
- Charles Riley, “Google urged to abandon Saudi cloud project,” *CNN*, May 26, 2021, <https://www.cnn.com/2021/05/26/tech/google-saudi-arabia-cloud/index.html>.

Notes

¹ Peter Jeydel, Ed Krauland, Meredith Rathbone, Guy Soussan, and Stefan Tsakanakis, “New Human Rights Licensing Policy under U.S. Export Controls – Convergence with the EU,” *Steptoe International Compliance Blog*, October 6, 2020, <https://www.steptoointernationalcomplianceblog.com/2020/10/new-human-rights-licensing-policy-under-u-s-export-controls-convergence-with-the-eu/>.