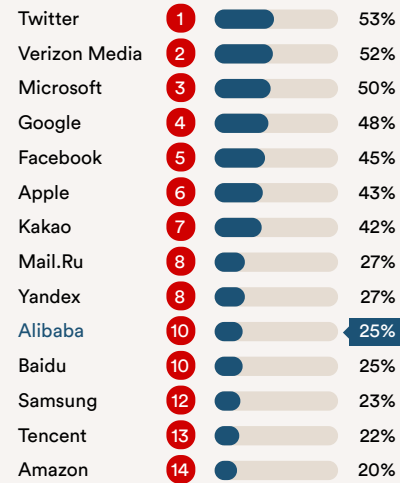


# Alibaba Group Holding Limited

Rank: **10th** Score: **25%**

Headquartered in China, Alibaba runs China's largest e-commerce platform, alongside other internet services ranging from cloud computing and office tools to video streaming and food delivery platforms. It has an annual active base of **780 million users** in China.



**New to the 2020 RDR Index, Alibaba was one of the lowest-scoring digital platforms in our ranking.** In 2020, in response to the COVID-19 pandemic, the Chinese government rolled out an algorithmically driven **health tracking system** as a way to monitor citizens and control the spread of the disease, leveraging technologies built by both Alibaba and Tencent and triggering public concerns around privacy rights. Like other Chinese companies, Alibaba said little about its policies for handling censorship and surveillance demands from Chinese authorities. China's political environment discourages companies from disclosing detailed information about these types of demands. Still, Alibaba earned a higher score on privacy than its direct peer, Amazon, and Russian companies Mail.Ru and Yandex. It was the only company in the entire RDR Index to clearly disclose it uses de-identified user information to train algorithms by default.

## Key takeaways

- Alibaba did not publish a commitment to respect users' rights to freedom of expression and privacy.
- Alibaba was one of the least transparent platforms regarding its handling of government demands for user information.
- While still falling short, Alibaba scored higher on privacy indicators than a number of other companies, including Amazon.

## Key recommendations

- Commit to respect human rights. Alibaba should make a formal commitment to respect freedom of expression and privacy as human rights.
- Clarify the process for responding to third-party demands. Alibaba should clarify its processes for responding to government demands to censor content and to hand over user information. While China's political environment discourages companies from disclosing detailed information about government requests for user information, Alibaba should be able to disclose if and when it shares user information via private requests and under what circumstances.
- Increase transparency of targeted advertising. Alibaba should publish its policies on targeted advertising and publish data on the enforcement of those rules.

#### Services evaluated:



Taobao.com



AliGenie

The 2020 RDR Index covers policies that were active between February 8, 2019 and September 15, 2020. Policies that came into effect after September 15, 2020 were not evaluated for this Index. Scores reflect the average score across the services we evaluated, with each service weighted equally.

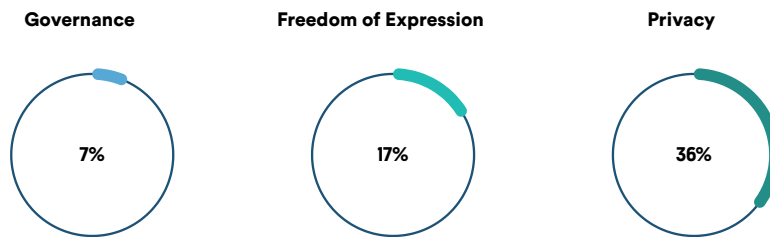
**Lead researchers:** Jie Zhang, Veszna Wessenauer

**Market cap:** \$713.1 billion (As of February 4, 2021)

**NYSE:** BABA

**Website:**

<https://www.alibabagroup.com>



We rank companies on their governance, and on their policies and practices affecting freedom of expression and privacy.

## Governance 7%

Alibaba received the third-lowest governance score among digital platforms, outperforming only Tencent and Amazon.

- **Commitment to human rights:** Alibaba did not disclose a commitment to protect users' freedom of expression and privacy rights (G1).
- **Human rights due diligence:** Alibaba offered no evidence that it conducts human rights impact assessments on any aspects of its business practices or policies (G4a-e).
- **Stakeholder engagement:** Alibaba provided no evidence of engaging with stakeholders whose rights are affected by the company's operations (G5).
- **Remedy:** Alibaba failed to provide a clear human rights grievance mechanism. According to the privacy policies of Taobao.com and AliGenie, users can submit questions, file complaints, or report data breaches, but it was not clear whether this remedy mechanism covers privacy-related complaints about the company's own policies. No remedy option was available for freedom of expression complaints (G6a). Taobao.com allowed users to appeal some content moderation actions and present additional information for review. The company disclosed no information about the time frame for notifying affected users (G6b).

## Freedom of Expression 17%

Alibaba disclosed little about policies affecting freedom of expression and information.

- **Content moderation:** Alibaba disclosed information about its content rules and how they are enforced (F3a). Taobao.com had a rolling "punish list" page publicizing the accounts of vendors who had been suspended or terminated each week for "releasing prohibited information," but this page did not address the volume of content removals and account deactivations that the company imposes based on its rules. AliGenie published no enforcement data whatsoever (F4a, F4b).
- **Algorithmic use and content curation:** Alibaba did not publish rules governing the use of algorithms on its services (F1d, F2d). While the privacy policy of Taobao.com offered users the ability to opt out of content curation and recommendation, the information provided was vague and did not explain clearly how algorithms were used for curating content on these services (F12).
- **Advertising content and targeting:** Alibaba's advertising content rules were scattered across multiple pages and policies and therefore not easy to find (F1b). Its advertising content rules clearly disclosed what types of ad content are prohibited, but the company did not reveal whether it required all advertising content to be labelled (F3b). The company did not explain how it enforces its ad targeting rules (F3c). Alibaba published no data about the enforcement of its ad policies (F4c).
- **Censorship demands:** Taobao's Market Management and Violation Punishment Regulation page outlined its process for responding to government demands and court orders (F5a). It also explained its process for handling private requests to restrict content or accounts (F5b). No such information was provided for AliGenie. The company did not publish any information about the number and volume of such requests it received or complied with (F6, F7). Although no specific laws or regulations in China prohibit Chinese companies from publishing data about government demands to restrict content, the political environment and controls over the internet make it almost impossible for Chinese companies to release such information.

## Privacy 36%

Alibaba revealed more information about its policies and practices affecting users' privacy than Mail.Ru, Yandex,

- **Handling of user data:** The company revealed some information about how it handles user information, including the types of information it collects (P3a), infers (P3b), and shares (P4). Alibaba was the only company in 2020 to clearly disclose that it uses de-identified user information to train algorithms by default (P7). However, it disclosed very little about its data retention policies (P6) and nothing about whether users can access information that the company holds about them (P8).
- **Government and private demands for user data:** Alibaba's Group-E-Commerce Platforms International Law Enforcement User Information Request Guide offered guidance for law enforcement agencies in foreign jurisdictions about how to request user information from Alibaba (P10a). But Alibaba did not disclose anything about its processes for handling demands from Chinese authorities (P10a) or any data about these types of demands it receives (P11a). Although there are no laws or regulations in China prohibiting Chinese companies from releasing data about government demands to access user information, the political environment discourages companies from doing so. Alibaba also failed to provide information about how it handles private demands for user information (P10b) or any data about these types of requests that it receives or complies with (P11b).
- **Security:** Alibaba's security policies were not comprehensive. Alibaba was one of the two most transparent digital platforms, along with Baidu, with regard to data breach policies (P15), as required under China's Cybersecurity Law.<sup>[1]</sup> Alibaba committed to notifying affected users and authorities about data breaches and shared the steps it would take in the event a breach occurred. But the company was less clear about its internal security protocols (P13). The company had a bug bounty program allowing external researchers to submit reports of security vulnerabilities, but it explicitly reserved the right to pursue legal action against researchers in certain cases (P14).
- **Encryption:** Alibaba encrypted the transmission of user communication. However, like its Chinese peers Baidu and Tencent, the company failed to provide end-to-end or full-disk encryption to secure users' private content. China's Cybersecurity Law<sup>[2]</sup> and Anti-Terrorism law<sup>[3]</sup> require internet operators to provide authorities with access to user communications to assist investigations (P16).

## Footnotes

[1] Article 42 of the Cybersecurity Law of PRC, [http://www.cac.gov.cn/2016-11/07/c\\_1119867116.htm](http://www.cac.gov.cn/2016-11/07/c_1119867116.htm). For the English translation, see: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>

[2] Article 28.

[3] Article 18 of the Anti-Terrorism Law of PRC, [http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content\\_2055871.htm](http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm). For the English translation, see: <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/>