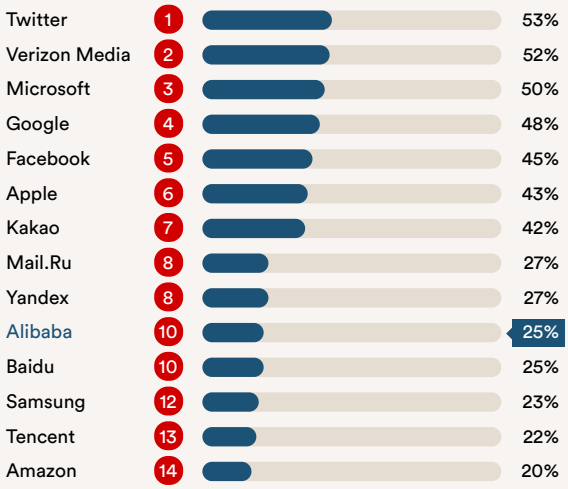
Digital platforms

Alibaba Group Holding Limited

Rank: 10th Score: 25%

Out of 14 digital platforms.

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. It was the only company that did not explicitly commit to respect users' privacy rights, though it did state that it "puts the user first" when it comes to data protection. 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 [LINK TO TENCENT CARD] and triggering public concerns around privacy rights. Like other Chinese internet companies, Alibaba does not maintain adequate transparency about its processes for handling government requests for content restrictions or user information, due primarily to China's tight controls over the internet and a series of laws and regulations affecting privacy and expression. Also in 2020, former U.S. Secretary of State Mike Pompeo called on U.S. tech companies to cut ties with their Chinese peers, including Alibaba. In response, Alibaba's chief executive Daniel Zhang emphasized the importance of the e-commerce platform for American brands, retailers, and small businesses. The antitrust campaign launched by Chinese government against China's Internet companies recently including Alibaba may stifle its growth but push it to act more transparently in the future.

Key takeaways

- Apple earned the highest privacy score of any digital platform we evaluated, and stood out for strong disclosure of its security policies.
- Apple lacked transparency about its process for removing apps from the App Store for violations to iOS rules.
- Apple lagged behind its peers on human rights due diligence, but strengthened its human rights commitments.

Key recommendations

- Be transparent about rules enforcement. Apple should publish data about actions it takes to enforce its own rules, including about apps removed from its App Store, and strengthen mechanisms to appeal enforcement decisions.
- Strengthen human rights due diligence. Apple should commit to conducting robust, systematic risk assessments on all aspects of its operations and business practices. The scope of these assessments should include evaluting risks to freedom of expression and information and the right to non-discrimination associated with the development and use of algorithmic systems and of its targeted advertising policies and practices.
- Increase user control. Apple should give users more options to control their own information. Targeted advertising should be *off* by default.

Services evaluated:

Taobao.com

AliGenie

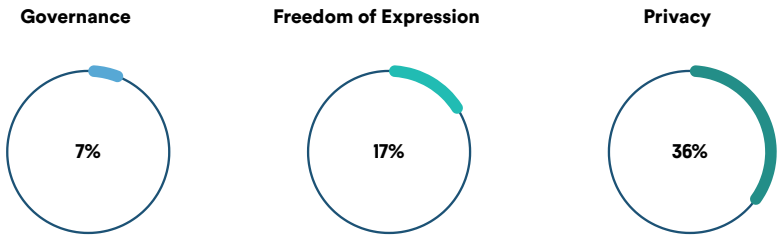
The 2020 RDR Index covers policies that were active between February 8, 2019 and September 15, 2020. Policies that came into effect after September 15, 2020 were not evaluated for this Index. Scores reflect the average score across the services we evaluated, with each service weighted equally.

Lead researchers: Jie Zhang, Veszna Wessenauer

Market cap: $713.1 billion (As of Feburary 4, 2021)

NYSE: BABA

Website:
https://www.alibabagroup.com



We rank companies on their approach to governance, and their policies and practices that affect freedom of expression and privacy.

Governance 7%

Apple ranked fifth among digital platform companies we evaluated, falling short on human rights due diligence in comparison to its U.S. peers.

- **Commitment to human rights:** Apple disclosed a clear and explicit commitment to protect and respect privacy and freedom of expression and information but failed to disclose a similar human rights commitment in its use and development of algorithmic systems (G1).
- **Human rights due diligence:** Apple disclosed it conducts limited assessments of privacy risks associated with government regulations in the markets in which it operates (G4a), but does not provide evidence of conducting due diligence in other areas, including of its own policy enforcement, on its development and use of algorithmic systems, or on targeted advertising.
- **Stakeholder engagement:** Apple failed to provide evidence of systematic engagement with stakeholders whose privacy and freedom of expression and information are directly impacted by the company (G5).
- **Remedy:** Apple disclosed little about its remedy mechanisms to address users' freedom of expression and information as well as privacy grievances (G6a) and even less about its processes for users and developers to appeal app removals from the App Store (G6b).

Freedom of Expression 17%

Apple lagged behind South Korea-based Kakao and most of its U.S. peers in this category.

- **Content moderation:** Apple did not clearly disclose platform rules and its process for enforcing them (F3a), including rules on bots (F13). Nor did it report any data about content removals and account suspensions for violations to these policies (F4a, F4b). It offered almost no information on whether or how it notifies users when content is removed (F8).
- **Algorithmic use and content curation:** Apple revealed nothing about how it uses algorithms to curate, rank, or recommend content in its App Store (F12).
- **Advertising content and targeting:** The company lacked transparency about its ad content and ad targeting rules and enforcement process (F3b, F3c), and it did not publish data on content removed for violating these rules (F4c).
- **Censorship demands:** Apple was transparent about its process for responding to government censorship demands (F5a) but disclosed very little about censorship requests submitted through private processes (F5b). For the first time, it reported the number of government takedown requests for apps in its App Store, and it listed associated subject matters, following through on a prior commitment to do so. It also began disclosing the number of App Store takedown requests from governments for alleged violations of Apple's own Terms of Service (F6), but none about private requests (F7).

Privacy 36%

Apple earned the highest privacy score, but fell short in key areas.

- **Handling of user data:** While Apple did disclose some information about what user data it collects and shares, and why, it did not disclose anything about its data inference policies (P3b). Apple remained the only platform in the RDR Index to disclose it does not track users around the web, but the company disclosed nothing about whether it collects information about users through third-party data brokers (P9).
- **Government and private demands for user data:** Apple was transparent about its process for responding to government demands for user information (P10a), but disclosed less information about user information requests submitted through private processes (P10b). It provided data about government demands (P11a), but like its U.S. peers, Facebook did not divulge the exact number of requests received for user data under the Foreign Intelligence Surveillance Act or National Security Letters, or the actions it took in response to these requests, since it is prohibited by law from doing so. It also committed to notify users when government entities demand access to their information (P12). It did not publish any data about private requests (P11b), nor did it commit to notify users when their information is requested through private processes (P12).
- **Security:** Apple disclosed more about its security policies than any other digital platform we evaluated. It was fully transparent about its internal processes for keeping user information secure (P13) and offered resources and tools to help users protect their security (P17, P18). It was less clear about its policies on data breaches (P15), and it disclosed limited information about how it addresses security vulnerabilities (P14).