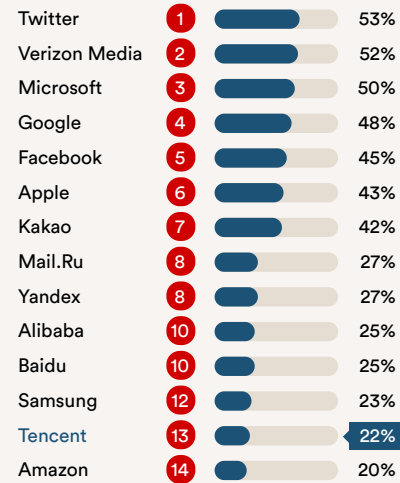


Tencent Holdings Limited

Rank: **13th** Score: **22%**

Headquartered in China, Tencent provides social media, messaging, gaming, music, and cloud services. Tencent's multi-purpose messaging platform, WeChat, dominates the Chinese market, with **1.2 billion**^[1] monthly active accounts held by government entities, businesses, media outlets, and individuals.



Tencent earned the second-lowest score among the 14 digital platforms in the RDR index, scoring lower than Baidu and Alibaba, the two other Chinese companies we rank. The Chinese government requires social platforms to filter and censor illegal content and material that is considered politically sensitive. In late 2019, a new regulation also required social platforms, including Tencent, to **use algorithms** to detect and remove banned content and promote ideas aligned with state and Communist party doctrine.^[2] This increased concerns about content moderation and privacy protection systems on WeChat, Tencent's "super app" that serves over one billion users as a messaging tool and primary online venue for news and information in China, as well as things like online payments. Independent research also showed that WeChat constantly surveilled and censored **private chats**, including those of its **international users**.

Key takeaways

- Tencent revealed less information about its governance and oversight over privacy and freedom of expression issues than any other digital platform in the RDR Index.
- Tencent published some data about accounts it restricted for violating the company's rules, but it failed to release any data about content restrictions to enforce its terms of service.
- Tencent shared little information about how it handled third-party demands, including relevant data about censorship and user information.

Key recommendations

- Conduct human rights due diligence. Tencent should conduct human rights due diligence, including by conducting risk assessments on new and existing services and when entering new markets.
- Publish data on content rule enforcement. Tencent should publish data about the volume of content it restricts for violating company rules to complement the data it publishes about account restrictions.
- Give users more control over their information. Tencent should provide users with more options to access and control their own information.

Services evaluated:



QZone



QQ



WeChat



Tencent Cloud

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, Zak Rogoff

Market cap: \$910.16 billion (as of February 4, 2021)

HKEX: 700

Website: <https://tencent.com>

Changes since 2019

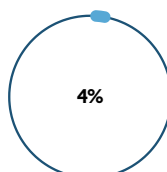
- Tencent increased its transparency about how it handled private requests to restrict or suppress content, including copyright claims.
- Tencent's QQ service published its own Privacy Protection Guidelines. The new policy included a clearer description of the service's data collection purposes and of what user data is collected from third parties. The policy also enabled users to delete some of the information the company collects about them, and it stated that the company has a dedicated team to conduct security audits.



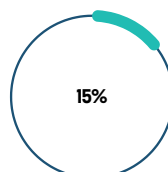
+ 1.38 points

Gained 1.38 points on comparable indicators since the 2019 RDR Index.

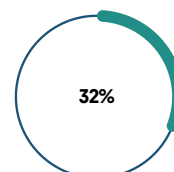
Governance



Freedom of Expression



Privacy



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

Governance 4%

Tencent disclosed little about its governance and oversight over human rights issues, revealing nothing except a commitment to protect users' privacy and a content moderation appeals mechanism for WeChat.

- **Commitment to human rights:** Tencent committed to protect users' information and privacy, but it did not identify privacy as a human right. It made no commitment to respect users' freedom of expression, nor did it commit to human rights in relation to its development and use of algorithms (G1).
- **Human rights due diligence:** Tencent disclosed no evidence of conducting any kind of human rights risk assessments (G4).
- **Stakeholder engagement:** Tencent provided no evidence of systematic engagement with stakeholders whose rights are directly affected by the company (G5).
- **Remedy:** Tencent did not provide users with mechanisms to seek remedy for freedom of expression or privacy grievances (G6a). WeChat offered users a relatively clear path to appeal content moderation decisions but disclosed incomplete information about its process and time frame. Tencent's other services failed to provide users with an effective appeals channel (G6b).

Freedom of Expression 15%

Tencent was one of the least transparent platforms that we evaluated when it came to policies and practices affecting users' freedom of expression and information, outperforming only Amazon and Baidu.

- **Content moderation:** In addition to a group terms of service, each of the services we evaluated had its own terms of service which offered reasons why Tencent might block content or accounts for violating company rules. The policies did not elaborate on the company's processes for identifying those violations and enforcing the rules (F3a). Through Tencent's security portal, the company published the total volume of accounts it had ever "punished" as well as monthly "crackdown" reports. While both these reports contained some data about accounts restricted for violating platform rules (F4b), they did not include any data about restrictions on content (F4a).
- **Algorithmic use and content curation:** Tencent failed to publish operational policies that govern the use or development of its algorithmic systems (F1d, P1d), but the company did reveal some information about the deployment of algorithmic systems for QQZone, a social networking and blogging service, to curate or recommend content. It did not provide users with the ability to control how these systems are deployed (F12).
- **Advertising content and targeting:** Tencent published rules that govern ad content and targeting on its ad services portal, but they were not easy to locate (F1b, F1c). The rules identified types of ad content that are prohibited on the platform, but they did not require all advertising content to be labelled as such (F3b). Tencent acknowledged that it allowed third parties to target users but failed to specify what targeting parameters were prohibited (F3c). Like most of its peers, the company failed to release data about ads removed for violating its rules (F4c).
- **Censorship demands:** Tencent did not offer any insight about its process for responding to government demands for content or accounts restriction, reflecting the political sensitivity of government censorship in China (F5a). But the company described some of the steps it followed in handling copyright-related private requests as well as the legal basis for such requests (F5b). Still, Tencent failed to release any data about either government or private demands to restrict content and accounts (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 discourages the release of such information.

Privacy 32%

Although Tencent shared some information that was relevant to protecting its users' privacy, the company had weak transparency about its security policies, as well as its processes for handling government and other types of third-party requests for user information.

- **Handling of user data:** Through its privacy portal, visitors could find key privacy information and all of Tencent's privacy policies (P1a). Tencent published more about how it collected user information and its purposes for collecting and inferring data than any other digital platforms in the RDR Index, although it did not commit to limiting the inference of user information to what was necessary for business purposes (P3, P5). Tencent did not release the names of any third parties with which it shared user information (P4), nor did it disclose how long it retained user information (P6). The company did not provide users with sufficient ways to control or access their own data (P7, P8).
- **Government and private demands for user data:** Tencent was one of the three digital platforms, in addition to Baidu and Samsung, that provided no information about its process for handling government demands to access user information (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. Tencent 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:** Tencent lacked transparency about its internal processes and practices to protect users' security, scoring above only Amazon and Samsung in this area. Although Tencent limited employees' access to user information, it was unclear if it monitored this access or if it conducted internal and external security audits regularly for all of its services (P13). The company had a security response center for researchers and others to report vulnerabilities, but it did not commit not to pursue legal actions against those who reported bugs (P14). As required by China's Cybersecurity law,^[3] Tencent established a policy to address potential data breaches, but it failed to clarify if it would report such breaches to the relevant authorities, which the law also requires (P15). Tencent was especially opaque about its encryption practices, which is unsurprising, given China's laws requiring internet operators to give authorities access to users' communications (P16).^[4]

Footnotes

[1] This figure combines users of the domestic and international versions of the tool. Tencent did not publish the volume of the monthly active users for each version separately.

[2] Article 12 of Provisions of Ecological Governance of Network Content, http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

[3] Article 42, Cybersecurity Law of PRC, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm; for English translation, see: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>

[4] Article 18, China Anti-Terrorism Law, http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm; and Article 28, Cybersecurity Law of PRC, http://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm