Telecommunications company

América Móvil, S.A.B. de C.V.

Operating company evaluated:

- **Telcel (Mexico)**

Services evaluated:

- **Telcel (Prepaid mobile)**
- **Telcel (Postpaid mobile)**

Rank	Score	Difference
7	25%	^ 3.39

Rank among 12 telecommunications companies

Key findings

- Despite some key improvements, América Móvil disclosed little about policies and practices affecting freedom of expression and privacy.
- América Móvil was unclear about its rules and how they are enforced, as well as how it responds to government requests to shut down networks.
- América Móvil did not clearly disclose how it handles government or private requests to block content or to hand over user information.

Key recommendations

- **Be transparent about external requests:** América Móvil should be more transparent about how it responds to government requests to block content, restrict user accounts, shut down networks, or hand over user information.
- **Improve human rights due diligence:** América Móvil should disclose information about its human rights due diligence processes, including whether it conducts human rights impact assessments.
- **Disclose more about security practices:** América Móvil should clarify its policies for securing user information, including its procedures for handling data breaches.

Analysis

América Móvil ranked seventh out of the 12 telecommunications companies evaluated, disclosing little about policies and practices affecting freedom of expression and privacy.[1] However, it improved its disclosure of governance and oversight over freedom of expression and privacy issues by making a formal commitment to respect users' freedom of expression and privacy rights.[2] It also disclosed new employee training and whistleblowing programs on human rights. Despite these improvements, América Móvil needs to disclose more to meet basic benchmarks for transparency in key areas. For instance, it did not disclose how it responds to government or private requests to block content or accounts, although no laws in Mexico prevent companies from doing so. In addition, although companies are required to report to the telecommunications authority how many government requests they received for real-time location tracking or access to user metadata, América Móvil did not publish this information.[3]

América Móvil, S.A.B. de C.V. offers telecommunications services in Mexico and 35 countries in the Americas and Europe. It offers mobile, fixed-voice, and data services and is one of the largest operators globally.

Market cap: USD 52.2 billion[4]
BMV: AMX L
Domicile: Mexico
Website: https://www.americamovil.com

Governance 37%

América Móvil scored below most of its peers in the Governance category, though it made some notable improvements. The company published a new human rights policy that articulates a clear commitment to respect users' human rights to freedom of expression and privacy (G1), and also disclosed new employee training and whistleblowing programs for reporting freedom of expression and privacy violations (G3). However, it continued to lack clear disclosure of whether it conducts human rights impact assessments, and failed to disclose if it assesses risks associated with its use of automated decision-making or targeted advertising (G4). It also failed to disclose a commitment to engage with a range of stakeholders on freedom of expression and privacy issues (G5). However, América Móvil offered better grievance and remedy mechanisms than most of its peers, enabling users to lodge freedom of expression and privacy related complaints, though it did not disclose its timeframe for these mechanisms or evidence that it is providing remedy (G6). Mexican companies are legally required to provide users with a complaint mechanism.[5]

Freedom of Expression 17%

América Móvil revealed little about policies and practices affecting freedom of expression, tying with Orange in this category and lagging behind Telenor, Vodafone, AT&T, and Telefónica. Telcel's terms of service were difficult to find and understand (F1), and lacked clarity about if and how it notifies users of changes (F2).[6] It disclosed some information about its process for enforcing its rules (F3) but failed to disclose any information about actions it took to block content or restrict user accounts for violating its rules (F4). América Móvil offered no information about how it handles government or private requests to restrict content or accounts (F5-F7). There are no laws in Mexico preventing the company from being more transparent about how it handles such requests.

In addition, it lacked clear disclosure about its network management policies (F9) and its approach to handling network shutdown requests from governments (F10). Although it published a policy on net neutrality principles, the operating company Telcel stated that it offers zero-rating for certain content on specific social networks and instant messaging services (F9).[7] Like many of its peers, América Móvil disclosed no information about how it responds to government demands to shut down networks (F10).

Privacy 26%

América Móvil failed to disclose sufficient information about policies and practices affecting privacy and security. Like most telecommunications companies, América Móvil provided almost no information about how it responds to third-party requests for user information (P10). Its score declined due to a change in disclosure which made it less clear if the company carries out due diligence before it responds to government requests for user information (P10). América Móvil failed to disclose whether it informs users when their information is requested (P12). It did not publish any data about such requests (P11), despite being required by law to report the number of government requests for real-time location tracking or user metadata to the country's telecommunications authority.

Telcel disclosed little about what types of user information it collects (P3), shares (P4), and its reasons for doing so (P5). Like most of its peers, Telcel disclosed nothing about its policies for retaining user information (P6), although no law prohibits the company from doing so. It disclosed little about options users have to control what information is collected, including for targeted advertising (P7).

While Telcel provided some information on its processes for securing user data, including limiting and monitoring employee access (P13), it failed to disclose any information about how it addresses security vulnerabilities, including if it offers a bug bounty program for security researchers to submit vulnerabilities (P14). Like most companies in the Index, Telcel disclosed nothing about its policies for addressing data breaches (P15). Companies in Mexico are legally required to notify users only if the data breach "significantly affects" their rights, however the company does not disclose this information to users.[8]

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] See América Móvil's performance in the 2018 Index: rankingdigitalrights.org/index2018/companies/americamovil

[3] "ACUERDO Mediante El Cual El Pleno Del Instituto Federal de Telecomunicaciones Expide Los Lineamientos de Colaboración En Materia de Seguridad Y Justicia Y Modifica El Plan Técnico Fundamental de Numeración, Publicado El 21 de Junio de 1996," (DOF - Diario Oficial de La Federación), www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

[4] Bloomberg Markets, Accessed April 18, 2019, https://www.bloomberg.com/quote/AMXL:MM

[5] LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, Última reforma publicada DOF 31-10-2017: www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_311017.pdf

[6] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Telcel (Mexico).

[7] "Política de Uso Justo/¿En qué consiste?," Telcel, accessed March 21, 2019, www.telcel.com/mundo_telcel/quienes-somos/corporativo/uso-justo

[8] "Ley Federal de Protección de Datos Personales En Posesión de Los Particulares," Article 20 (2010), www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Internet and mobile ecosystem companies

Apple, Inc.

Services evaluated:

- **iMessage [Messaging & VoIP]**
- **iCloud [Cloud service]**
- **iOS [Mobile ecosystem]**

Rank	Score	Difference
7	46%	^ 1.47

Rank among 12 internet and mobile ecosystem companies

Key findings

- Apple had strong disclosure of privacy and security policies, but only limited disclosure of policies and practices affecting freedom of expression.
- Apple disclosed little about its rules and how they are enforced, and revealed no data about content removed—including apps removed from its App Store—as a result of government requests.
- It was the only company in the Index to clearly disclose it does not track users across third-party websites, and disclosed more about its encryption policies than all of its peers.

Key recommendations

- **Improve governance and oversight:** Apple should disclose a commitment to respect freedom of expression as a human right, and put processes in place to strengthen institutional oversight over freedom of expression issues at the company.
- **Be transparent about restrictions to freedom of expression:** Apple should make its terms of service easier to find and understand. It should publish data about actions it takes to enforce its own rules and actions it takes to remove content as a result of government and other third party demands.
- **Clarify handling of user information:** Apple should clarify what types of user information it collects, shares, and retains, and for what purposes.

Analysis

Apple placed seventh among the 12 ranked internet and mobile ecosystem companies in the 2019 Index.[1] As in previous Index rankings, Apple's low score relative to its U.S. peers was due to its lack of governance and oversight over human rights risks, and also lack of clear disclosure of policies affecting users' freedom of expression.[2] On privacy and security issues, Apple remains near the top of all ranked companies in this Index. It was the only company to clearly disclose it does not track users across the internet, and disclosed more about its encryption policies than its peers. For its mobile operating system, Apple also disclosed more than Google's Android and Samsung's Android about options users have to control location tracking on iOS.

But Apple should be more transparent and accountable to users about policies and practices that affect freedom of expression: Of the user agreements evaluated in the RDR Index, Apple's were among the least accessible. It also lacked adequate disclosure about its rules and how they are enforced. While it disclosed data about government requests to restrict accounts, it disclosed no data about content removal requests, such as requests to remove apps from its App Store.

Apple, Inc. manufactures computers, smartphones, and other devices, and also produces iOS operating system software and application software.

Market cap: USD 957.8 billion[3]
NasdaqGS: AAPL
Domicile: USA
Website: https://www.apple.com

Governance 32%

For the third year in a row, Apple had the lowest governance score of any U.S. company evaluated in the Index. It disclosed a clear commitment to respect privacy as a human right (G1) but made no such commitment to freedom of expression. Apple clearly stated that senior leadership exercises oversight over how its policies and practices affect privacy (G2) but failed to reveal if there is similar oversight over freedom of expression issues. Apple disclosed that it assesses privacy risks associated with new products and services, however, it did not disclose if it assessed risks regarding its use of automated decision-making or targeted advertising (G4). Like most of its peers, Apple disclosed little about its grievance and remedy mechanisms for users to submit complaints against the company for infringement of their freedom of expression or privacy (G6).

Freedom of Expression 33%

Apple revealed little about policies and practices affecting freedom of expression, scoring below all other U.S. companies in this category. Apple's user agreements for the services evaluated were the least accessible of all other internet and mobile ecosystem companies (F1)—including the Chinese and Russian companies—and did not specify if and how it notifies users of changes to these terms (F2). Apple also disclosed less than all other U.S. internet and mobile ecosystem companies about its rules and processes for enforcing them (F3, F4, F8). While it provided some information about what content and activities are prohibited across its services (F3), Apple disclosed no data about content it removed or accounts it deactivated as a result of violations of these rules (F4).

Apple was less transparent about external requests to restrict content or accounts than most of its U.S. peers, except for Facebook (F5-F7). It only disclosed data about the number of government requests to restrict or delete accounts that it received, but gave no data about content removed as a result of these requests, including data about apps removed from its App Store (F6). Like many companies, Apple failed to provide any information or data about content and account restriction requests it received through private processes (F7).

Privacy 58%

Apple tied with Google for the second-highest score (after Microsoft) in the Privacy category, and had especially strong disclosure of its security policies. Like most of its peers, Apple fell short of clearly explaining how it handles user information, disclosing less than Twitter, Google, Verizon Media, and Facebook (P3-P9).[4] It did not fully disclose each type of user information it collects (P3), shares (P4), for what purpose (P5), and for how long it retains it (P6). However, Apple was the only company in the Index to clearly disclose that it does not track users across third-party websites (P9).

Apart from Google and Microsoft, Apple was more transparent than other internet and mobile ecosystem companies about its process for handling government and other external requests for user information (P10-P12). It disclosed some information about its process for responding to government requests but no similar disclosure could be found regarding the private requests it received (P10). Apple tied with Twitter and Facebook for its disclosure of data about third-party requests for user information it received and complied with (P11). Like other U.S. companies, Apple did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.[5]

Apple disclosed more than any other internet and mobile ecosystem company about its security policies, but still fell short in key areas. It disclosed some information about its internal security oversight processes but provided no information about whether it commissions external security audits on its products and services (P13). However, it made notable improvements to its disclosure of how it encrypts user communications for iOS, iMessage, and iCloud (P16).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Apple's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/apple

[3] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/AAPL:US

[4] Oath, which provided a range of communications services including Yahoo Mail and Tumblr, updated its name to Verizon Media on January 7, 2019. See: www.oath.com/2019/01/07/oath-is-now-verizon-media

[5] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Telecommunications company

AT&T Inc.

Services evaluated:

- **AT&T [Prepaid mobile]**
- **AT&T [Postpaid mobile]**
- **AT&T [Fixed-line broadband]**

Rank	Score	Difference
3	48%	0

Rank among 12 telecommunications companies

Key findings

- AT&T had weak governance and oversight over human rights issues and ranked third among telecommunications companies, disclosing less about policies affecting privacy and freedom of expression than Telefónica and Vodafone.
- It had especially unclear disclosure of its network management policies, and offered zero rating programs that undermine net neutrality.
- AT&T had relatively strong disclosure of policies affecting privacy but still did not disclose enough about its handling of user information.

Key recommendations

- **Clarify handling of user information:** AT&T should clarify what types of user information it collects, shares, and retains, and for what purposes.
- **Commit to net neutrality in practice:** AT&T should affirm its commitment to upholding net neutrality principles by refraining from engaging in paid prioritization of traffic, including offering zero rating programs—a form of network discrimination that undermines net neutrality in practice.
- **Clearly communicate security practices:** AT&T should clearly inform users about its policies for responding to data breaches.

Analysis

AT&T has consistently landed among the top-scoring telecommunications companies in the RDR Index, but dropped to third place in this year's ranking, after Telefónica and Vodafone.[1] AT&T is not a member of the Global Network Initiative (GNI)—the company did not join the multi-stakeholder organization in 2017 when many of its European telecommunications peers did—and has since lagged behind many GNI-member companies in key areas.[2] It had weak governance and oversight over human rights issues as compared to GNI members. The company also fell short of disclosing policies affecting freedom of expression. Notably, AT&T's network management policies and commitments were unclear: it committed to not prioritize certain types of network traffic over others, but also offered zero rating programs, a form of network discrimination which undermines net neutrality in practice.[3] While it had relatively strong disclosure of policies affecting user privacy, it could be far more transparent about data collection, sharing, and retention policies and practices.

AT&T Inc. provides telecommunications services in the United States and in Mexico, offering data and voice services to approximately 170 million wireless subscribers.[4]

Market cap: USD 232.7 billion[5]
NYSE: T
Domicile: USA
Website: https://www.att.com

Governance 60%

AT&T disclosed less about its governance and oversight over human rights issues than Telefónica, Vodafone, Orange, and Telenor. It published a formal human rights policy that clearly articulates the company's commitment to upholding users' freedom of expression and privacy rights (G1), but disclosed almost nothing about its human rights due diligence efforts that would enable the company to anticipate and mitigate harms (G4). AT&T failed to disclose if it conducts risk assessments on existing products and services, its terms of service enforcement, or its use of automated decision-making and targeted advertising (G4). It also disclosed little evidence of stakeholder engagement on digital and human rights issues (G5). Like most companies in this Index, AT&T failed to disclose much information about its grievance and remedy mechanisms for users to lodge complaints when they feel their freedom of expression or privacy has been violated by the company (G6).

Freedom of Expression 40%

AT&T disclosed more about policies affecting freedom of expression than most other telecommunications companies evaluated, apart from Telefónica and Vodafone—but still lacked transparency in key areas. It disclosed little to no information about actions it took to block content or restrict user accounts, either as a result of breaches to the company's own rules (F4) or from government or other types of third-party requests (F6, F7). While AT&T was among only three telecommunications companies in the RDR Index to report any data about compliance with government demands (F6), it could be more transparent with users in this area. It also disclosed nothing about private requests to block content or deactivate accounts (F7).

The company's network management policies and practices were also unclear (F9). Following the repeal of the FCC's Open Internet Order in late 2017, AT&T announced plans to move forward with paid prioritization for certain types of traffic—which directly undermines net neutrality—but also claimed it "was not interested in creating fast lanes and slow lanes."[6] In its public disclosure evaluated for the RDR Index, AT&T committed to not prioritize certain types of network traffic over others, but at the same time offered a zero rating program, a form of network discrimination which undermines net neutrality in practice (F9). The company also disclosed almost nothing about its policies for handling government demands to shut down a network, although it did clarify that it would report the number of government requests to shut down its networks if it received such requests (F10).

Privacy 49%

AT&T tied with Telefónica for the second-highest privacy score after Deutsche Telekom. The company revealed more than all of its peers about its handling of government requests for user information (P10, P11) but lacked disclosure of its handling of user information (P3-P8). It revealed more about what types of user information it collects (P3), than about what it shares with whom (P4) and why (P5)—and revealed almost nothing about its data retention policies (P6). Like all telecommunications companies, AT&T failed to indicate if it notifies users about government or other types of third-party requests for their information (P12). It also did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.[7]

AT&T was one of the few telecommunications companies to fully disclose its policies for securing user data (P13), and that it has a bug bounty program to help identify and remedy security vulnerabilities (P14). But the company lacked clarity about its policies for handling data breaches (P15).

Footnotes

[1] For AT&T's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/att

[2] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[3] Sponsored Data, AT&T, www.att.com/att/sponsoreddata/en/index.html

[4] "3Q 2018 AT&T by the Numbers" (AT&T, 2018), www.att.com/Common/about_us/pdf/att_btn.pdf

[5] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/T:US

[6] Bob Quinn, "Let's Take Action and Enact a Federal Consumer Bill of Rights," February 27, 2018, www.attpublicpolicy.com/consumer-broadband/lets-take-action-and-enact-a-federal-consumer-bill-of-rights/

[7] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Telecommunications company

Axiata Group Berhad

Operating company evaluated:

- **Celcom (Malaysia)**

Services evaluated:

- **Celcom (Prepaid mobile)**
- **Celcom (Postpaid mobile)**

Rank	Score	Difference
10	14%	0

Rank among 12 telecommunications companies

Key findings

- Axiata made modest improvements but remained one of the lowest-ranking companies in the entire Index.
- Axiata disclosed nothing about how it responds to government or private requests to block content, restrict accounts, or hand over user information.
- While Axiata made minor improvements to its privacy policies, it was less transparent than previously about its security policies.

Key recommendations

- **Be more transparent about external requests:** Axiata should be clear about how it responds to government and private requests to block content, restrict accounts, or hand over user information.
- **Communicate more clearly about security:** Axiata should disclose details about how it secures user information, including how it responds to data breaches.
- **Improve disclosure about network shutdowns:** Axiata should clarify how it handles government orders to shut down networks, including by committing to push back against these types of demands.

Analysis

Axiata ranked tenth out of 12 telecommunications companies evaluated, disclosing less than most of its peers about policies and practices affecting freedom of expression and privacy.[1] The company strengthened its disclosure of governance and oversight over privacy issues and improved its disclosure across a number of policies affecting users' privacy.[2] However, despite these improvements, Axiata's overall score remained the same because of declines to its disclosure of its security policies. The company operates in a challenging regulatory environment, and Celcom, Axiata's operating company in Malaysia, must comply with regulations from the Malaysian Communications and Multimedia Commission (MCMC) and other authorities.[3] But there are no laws preventing Celcom from making basic commitments to respect users' freedom of expression and privacy, nor are there any legal obstacles preventing Axiata from improving its disclosure of how it handles user information. While Malaysia's Official Secrets Act may prohibit some disclosure of government requests, nothing prevents Celcom from publishing at least some information about these types of third-party requests for user information.[4]

Axiata Group Berhad provides telecommunications and network transmission related services to almost 300 million mobile subscribers in markets across Asia.[5]

Market cap: USD 8.9 billion[6]
KLSE: AXIATA
Domicile: Malaysia
Website: https://www.axiata.com

Governance 9%

Despite some improvements, Axiata disclosed less about its governance and oversight over freedom of expression and privacy issues within the company than all other telecommunications companies evaluated, aside from Etisalat and Ooredoo. It did not publish a commitment to respect users' freedom of expression and privacy as human rights (G1). Axiata improved its disclosure of executive-level oversight over privacy issues (G2) and clarified that employees can report privacy-related concerns under its whistleblowing policy (G3), although it was not clear whether the policy covered all types of privacy-related issues. The company did not publish any information about conducting human rights impact assessments (G4). It offered mechanisms for users to submit complaints related to privacy (G6), but did not provide any information on how it responds to these complaints.

Freedom of Expression 13%

Axiata disclosed minimal information about its policies affecting freedom of expression and tied with Ooredoo for the second-lowest score among telecommunications companies, ahead of MTN and Bharti Airtel. The operating company, Celcom, offered terms of service that were easy to find but not so easy to understand (F1), and it failed to commit to notify users in cases of changes to the terms (F2).[7] Like most telecommunications companies evaluated, Celcom provided insufficient information about its network management and shutdown policies (F9, F10). It disclosed that it may block or delay certain types of traffic and applications for the purpose of minimizing the impact of heavy usage on its networks (F9). Notably, Axiata disclosed almost nothing about how it handles government demands to shut down its networks: it failed to provide any information about its process for responding to such demands, including whether it commits to push back against inappropriate demands or notify users when it shuts down service (F10).

Axiata otherwise earned no credit on any of the other indicators in the Freedom of Expression category. It was among seven telecommunications companies that disclosed nothing about processes for responding to third-party requests for content and account restrictions (F5) and published no data about the number of requests it received or with which it complied (F6, F7).

Privacy 16%

Axiata failed to disclose sufficient information about policies and practices affecting the privacy and security of its users, outperforming only MTN, Etisalat, and Ooredoo. Celcom published a privacy policy that was easy to locate and easy to understand (P1); however, unlike in previous years, it was no longer available in the primary languages of the company's home market. It provided less information than most telecommunications companies evaluated about how it handles user information (P3-P8). It offered users no information about how long it retains user information (P6), options to control what information the company collects about them (P7), or options to obtain the information the company holds on them (P8), and its disclosure of what information it collects (P3), shares (P4), and why (P5) fell short. Celcom improved its disclosure by stating that it may combine user information across different services (P5), although it did not specify which types of user information.

Axiata disclosed nothing about how it handles third-party requests to hand over user information, nor did it publish any data on the requests it received or with which it complied (P10, P11). Like all other telecommunications companies, it failed to commit to notify users if their information is requested by third parties (P12). There are no laws that prevent Axiata from being more transparent about these processes. Celcom also disclosed little about its security policies. It provided less detail than in the previous year about limiting employee access to user information (P13) or about how users can protect themselves from security risks (P18). It did not publish anything on how it addresses security vulnerabilities (P14) or how it responds to data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Axiata's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/axiata

[3] "Freedom on the Net," (Freedom House, November 2018), freedomhouse.org/report/freedom-net/2018/malaysia

[4] "Official Secrets Act 1972," Act 88 (1972), www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%2088.pdf

[5] "Key Highlights," Axiata Group Berhad, Accessed January 15, 2019, www.axiata.com/corporate/key-highlights/

[6] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/AXIATA:MK

[7] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Celcom.

Internet and mobile ecosystem companies

Baidu, Inc.

Services evaluated:

- **Baidu Search** [Search engine]
- **Baidu Cloud** [Cloud service]
- **Baidu PostBar** [Social networking & blog]

Rank	Score	Difference
11	23%	^ 6.21

Rank among 12 internet and mobile ecosystem companies

Key findings

- Despite having the second highest score-improvement of all companies in the 2019 RDR Index, Baidu had the second-lowest overall score among internet and mobile ecosystem companies.
- Baidu disclosed little about how it safeguards users' right to freedom of expression, but made significant strides in disclosures regarding its respect of users' privacy rights.
- Baidu disclosed nothing about its process for responding to third-party requests to restrict access to content or accounts, and published no data about these types of restrictions.

Key recommendations

- **Improve disclosure of human rights due diligence:** Baidu should disclose more information about its human rights due diligence, including whether it conducts human rights risk assessments on new and existing services and when entering new markets.
- **Increase transparency about private requests:** Baidu should publish data about private requests to restrict content or accounts and for user information.
- **Improve user control of personal data:** Baidu should improve users' options to control and access their own information, including how that information is used for targeted advertising.

Analysis

Baidu earned the second-lowest score of all internet and mobile ecosystem companies, outperforming only Mail.Ru.[1] However, Baidu significantly improved its disclosure of how it handles user information, and earned the second-highest score improvement of all companies evaluated.[2] Baidu improved the accessibility of its privacy policy, provided more detailed information on its data sharing policies—including the types of user information it shares and for what purposes—and improved its disclosure of options users have to obtain a copy of their own information. This progress could be attributed, in part, to new regulations requiring companies to be more transparent about their purposes for processing data.[3] However, the company still failed to meet basic standards for respecting users' freedom of expression and privacy. While the Chinese internet environment is restrictive, there are no legal barriers to prevent Baidu from further improving its policies for handling and securing user information.[4]

Baidu, Inc. provides internet search, cloud storage, social networking, and other services in China and internationally.

Market cap: USD 59.5 billion[5]
NasdaqGS: BIDU
Domicile: China
Website: https://www.baidu.com

Governance 7%

Baidu received the third-lowest governance score among all internet and mobile ecosystem companies, outperforming only Russian company Mail.Ru and Tencent, the other Chinese company included in the RDR Index. The company made a commitment to respect users' privacy and personal information, although it fell short of committing to respect privacy as a human right (G1). Baidu improved its disclosure by committing to provide employee training on privacy-related issues (G3). It did not disclose any information about conducting human rights impact assessments, including whether or not it assesses freedom of expression and privacy risks associated with its automated decision-making and its targeted advertising policies and practices (G4). It offered a complaints mechanism for PostBar users to submit freedom of expression and privacy related grievances, but not for its other services evaluated (G6). China's political and legal environment strongly discourages companies from making human rights commitments, but Baidu could still improve its disclosure of its grievance and remedy mechanisms (G6).

Freedom of Expression 12%

Baidu disclosed little about policies and practices affecting freedom of expression, revealing less than any other internet and mobile ecosystem company evaluated, including its Chinese peer, Tencent. While Baidu published terms for its services that were easy to find and relatively easy to understand (F1), it failed to disclose if and how it notifies users when it introduces changes to these terms (F2). It disclosed limited information about what types of content and activities are prohibited on its services (F3) and offered no data about the volume and nature of content or accounts it restricted for violating these rules (F4). It also did not commit to notify users when it restricts their access to content or accounts (F8).

Along with Samsung, Baidu was one of only two internet and mobile ecosystem companies that did not disclose any information about content and account restrictions in response to third party requests (F5-F7). It did not disclose any information about its process for responding to government or private requests to restrict content or accounts (F5), nor did it publish data about the requests it received and with which it complied (F6, F7).

Privacy 33%

Baidu disclosed less than most of the internet and mobile ecosystem companies in this category, despite improvements. It disclosed minimal information about how it handles user data (P3-P9), disclosing nothing about how long it retains user information (P6) or whether it tracks users across third-party websites and apps (P9). However, it improved its disclosure of its data sharing policies, including the types of user information it shares and with whom (P4) and for what purposes (P5), and of options users have to obtain a copy of their user information (P8).

Baidu disclosed little about how it handles government and private requests for user information (P10, P11), but disclosed more than Tencent. It improved disclosure of its policies of notifying users of third-party requests for user data (P12) by disclosing the circumstances under which it may not notify users, but failed to reveal any data about such requests (P11). Although the Chinese legal and political environment makes it unrealistic to expect companies to disclose detailed information about government requests, Baidu should be able to reveal if and when it shares user information via private requests and under what circumstances.

Baidu disclosed less information about its security policies (P13-P18) than all internet and mobile ecosystem companies aside from Samsung. It significantly improved its disclosure of how it responds to data breaches (P15) and improved its disclosure of limits on employees' access to user data (P13), but still failed to disclose any other information about its measures to keep user data secure (P13). It disclosed a bug bounty program through which security researchers can report vulnerabilities, but not a time frame in which it will review these reports (P14). It also disclosed that it uses encryption technologies (P16), but did not specify what types of data are encrypted and how.

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Baidu's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/baidu

[3] "Personal Information Security Specification," December 2017, www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE

[4] "Freedom on the Net - China" (Freedom House, November 2018), freedomhouse.org/report/freedom-net/2018/china

[5] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/BIDU:US

Telecommunications company

Bharti Airtel Limited

Operating company evaluated:

- **Airtel India**

Services evaluated:

- **Airtel India [Prepaid mobile]**
- **Airtel India [Postpaid mobile]**
- **Airtel India [Fixed-line broadband]**

Rank	Score	Difference
8	16%	^ 2.86

Rank among 12 telecommunications companies

Key findings

- Bharti Airtel disclosed little about its policies and practices affecting freedom of expression and privacy, and lacked disclosure of governance and oversight over human rights issues.
- It disclosed minimal information about how it enforces its rules, and no information about its process for responding to government or other types of third-party requests to restrict content or accounts.
- While it revealed some information about its policies for collecting and sharing user information, it revealed few details about how it responds to third-party requests for user data, and nothing about how it addresses security vulnerabilities or responds to data breaches.

Key recommendations

- **Improve governance of human rights:** Bharti Airtel should improve its governance and oversight over human rights issues, particularly over how its policies and practices affect freedom of expression.
- **Be transparent about network shutdown demands:** Bharti Airtel should disclose more about how it responds to government demands to shut down its networks.
- **Clarify security policies:** Bharti Airtel should disclose more about its security policies and practices, including how it responds to data breaches and addresses security vulnerabilities.

Analysis

Bharti Airtel ranked eighth out of the 12 telecommunications companies evaluated, disclosing less than most of its peers about policies and practices affecting freedom of expression and privacy.[1] While the company made several notable improvements this year—including publishing a new human rights policy—it still failed to disclose enough about its policies and practices affecting users' freedom of expression and privacy for users to have a clear sense of the risks of using the company's services.[2] It fell especially short around policies affecting freedom of expression and continued to disclose less than other telecommunications companies in the Index, except MTN. Freedom House rated the internet environment in India as "Partly Free," noting a "staggering increase" in the number of government orders to shut down networks.[3] Still, the company disclosed little about its policies for responding to these types of government demands. While Indian law prevents companies from disclosing information about specific government content restriction and shutdown orders, there are no legal obstacles preventing companies from disclosing policies for responding to these requests or from having a policy of notifying users about them.

Bharti Airtel Limited provides telecommunications systems and services worldwide, including in India, South Asia, and Africa. It delivers a variety of fixed and mobile voice and data telecommunications services.

Market cap: USD 20.1 billion[4]
BSE: 532454
Domicile: India
BSE: https://www.airtel.in

Governance 24%

Despite some improvements, Bharti Airtel scored poorly in this category, placing in the bottom half of all telecommunications companies evaluated. It disclosed a new commitment to respect users' human rights (G1), disclosed evidence of board-level oversight over how the company's operations and practices affect privacy (G2), and clarified that it has a whistleblower program that enables employees to report concerns about privacy-related issues (G3). However, the company disclosed no evidence that it conducts human rights impact assessments (G4). The operating company Airtel India[5] disclosed grievance mechanisms for users to submit freedom of expression and privacy complaints, as Indian law requires service providers to have grievance officers and redress mechanisms in place.[6] It also provided some information about its process for providing remedy for privacy concerns, but not those related to freedom of expression (G6).

Freedom of Expression 9%

Bharti Airtel tied with MTN for the lowest score of all telecommunications companies in this category, disclosing very little about its policies affecting users' freedom of expression. Airtel India published terms of service that were relatively easy to locate but not easy to understand (F1), and it failed to commit to notify users when it introduces changes to the terms (F2). It disclosed little information about its network management policies (F9) or about its policies and practices related to network shutdowns (F10). It provided some information about why it may shut down its network, but failed to disclose any information about its process for responding to government shutdown demands, or the number of requests it received or with which it complied (F10). While Indian law prevents companies from disclosing information about specific government shutdown orders, there is no legal obstacle to disclosing company policies for evaluating and responding to shutdown requests, or from having a policy to notify users about shutdowns.

Bharti Airtel disclosed nothing about how it handles and complies with government and private requests to restrict content or accounts (F5-F7). Indian law forbids disclosure of specific government orders to block content, but nothing prevents companies from disclosing their processes for handling these types requests (F5), or from having a clear policy to notify users when they restrict access to content or accounts (F8).[7]

Privacy 19%

Bharti Airtel disclosed little about policies affecting users' privacy rights, disclosing more than only Axiata, MTN, Etisalat, and Ooredoo. Airtel India's privacy policy was easy to find, but it was not available in Hindi nor was it presented in an understandable manner (P1). The company failed to commit to notify users when it introduces changes to the policy (P2). It disclosed less than most other telecommunications companies about how it handles user information, but more than MTN South Africa, Etisalat UAE, and Ooredoo Qatar (P3-P8). It disclosed some information about what types of user data it collects, shares, and for what purpose (P3, P4, P5), but nothing about how long it retains the information (P6). The company also failed to disclose whether it enables users to control what information about them is collected and shared, or if users can obtain the information Airtel India holds about them (P7, P8).

Bharti Airtel disclosed almost nothing about how it handles government and private requests for user information (P10-P11). Indian law prevents companies from publishing data on government requests for user information but does not prevent them from disclosing their processes for responding to the requests. Airtel India also disclosed little about its policies for securing user information (P13-P18). While it disclosed that it monitors and limits employee access to user information, it lacked clear disclosure of whether it conducts internal and external audits (P13). It provided no information at all about how it addresses security vulnerabilities (P14) or about how it responds to data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Bharti Airtel's performance in the 2018 Index, see: https://rankingdigitalrights.org/index2018/companies/bhartiairtel

[3] India report, Freedom on the Net 2018, Freedom House, freedomhouse.org/report/freedom-net/2018/india

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/BHARTI:IN

[5] For some indicators, RDR evaluates the operating company of the home market, in this case Airtel India.

[6] "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" (Ministry of Communications and Information Technology, April 11, 2011), meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

[7] "Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009" The Centre for Internet & Society, cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009

Telecommunications company

Deutsche Telekom AG

Operating company evaluated:

- **Deutsche Telekom Germany**

Services evaluated:

- **Deutsche Telekom Germany [Prepaid mobile]**
- **Deutsche Telekom Germany [Postpaid mobile]**
- **Deutsche Telekom Germany [Fixed-line broadband]**

Rank

5

Score

44%

Rank among 12 telecommunications companies

Key findings

- Deutsche Telekom earned the highest privacy score in the Index, disclosing significantly more than other telecommunications companies about policies affecting users' privacy.
- It failed to disclose adequate information about policies and practices affecting users' freedom of expression, including how it handles government demands to block or filter content or deactivate accounts.
- It also lacked strong governance and oversight over human rights issues relative to its European telecommunications peers.

Key recommendations

- **Be transparent about policies affecting freedom of expression:** Deutsche Telekom should be far more transparent about its policies affecting users' freedom of expression by clarifying its rules and processes for responding to government and other third party demands to block content or accounts.
- **Improve governance of freedom of expression commitments:** Deutsche Telekom should strengthen its governance and oversight over freedom of expression issues, including by disclosing evidence of senior-level oversight over these issues across the company's operations.
- **Clarify security policies:** Deutsche Telekom should publish more information on how it addresses security vulnerabilities and how it responds to data breaches.

Analysis

Deutsche Telekom ranked fifth out of the 12 telecommunications companies evaluated, scoring lower than Telefónica, Vodafone, AT&T, and Telenor.[1] The company—a newcomer to the RDR Index—earned the highest privacy score of any company evaluated, but lacked transparency about its policies affecting users' freedom of expression. Deutsche Telekom is the only European telecommunications company in the RDR Index that is not a member of the Global Network Initiative (GNI). As such, Deutsche Telekom lacked evidence of strong governance and oversight over human rights issues relative to its European peers in the RDR Index (Orange, Telefónica, Telenor, and Vodafone). Still, it disclosed significantly more about its policies affecting privacy than any company in the RDR Index, and in ways that surpassed its obligations under the EU's General Data Protection Regulation (GDPR).

Deutsche Telekom AG offers mobile, broadband, and other services in Europe, Africa, Asia, and the Americas.

Market cap: USD 79.5 billion[2]
Xetra: DTE
Domicile: Germany
Website: https://www.telekom.com

Governance 55%

Deutsche Telekom lacked strong governance and oversight over human rights issues—and in particular over freedom of expression—and scored lower than all other European telecommunications companies in this category. While it published a clear commitment to respect users' freedom of expression and privacy rights in accordance with international human rights standards and principles (G1), it only disclosed evidence of senior-level oversight over privacy issues but not freedom of expression (G2). Likewise, it clearly disclosed employee training and whistleblower programs for privacy issues, but left unclear whether the scope of those programs covered freedom of expression (G3). Deutsche Telekom was one of the few companies in the RDR Index (along with Microsoft and Telefónica) to disclose that it conducts impact assessments associated with its use of automated decision-making technologies—but focused on identifying impacts on users' privacy rights and not on freedom of expression rights (G4). It disclosed mechanisms for users to submit freedom of expression and privacy related complaints, but did not clarify its process for providing remedy and offered little evidence it was responding to these complaints (G6).

Freedom of Expression 15%

Deutsche Telekom failed to disclose adequate information about policies and practices affecting users' freedom of expression, and was among the least transparent of any company in the RDR Index. The company disclosed little about what types of content or activities are prohibited across its services (F3) and provided no data about any actions it took—such as blocking content or disabling accounts—due to user violations of rules (F4). Like most of its peers, Deutsche Telekom disclosed almost nothing about how it handles government or other types of third-party requests to restrict content and accounts (F5-F7): it disclosed nothing about its process for responding to government requests (F5), and provided no data about the number of these requests it complied with (F6-F7)—although there appear to be no legal reasons prohibiting the company from being more transparent.

Deutsche Telekom also disclosed nothing about its network management policies, and failed to publish a commitment to not prioritize certain types of traffic, applications, protocols, or content over others (F9). It disclosed minimal information about the reasons it may restrict access to its networks or specific applications (F10), but did not provide any additional details, including whether or not it commits to push back on government shutdown requests, or if it notifies users when it restricts their access to the network or a service.

Privacy 60%

Deutsche Telekom earned the highest privacy score in the RDR Index, disclosing significantly more than other telecommunications companies. It was far more transparent than any other telecommunications company about how it handles user information (P3-P8), clearly disclosing the types of user information it collects (P3), shares (P4), and its reasons for doing so (P5). It disclosed more about its data retention policies than any of its peers (P6). It was the only company in the Index to clearly disclose that targeted advertising is off by default, and that users can control how the company uses their information to deliver targeted ads (P7). However, it disclosed limited options for users to delete their information and no options at all for them to control the information that Deutsche Telekom collects on them (P7).

Deutsche Telekom also had relatively strong disclosure of how it responds to government and private requests for user data (P10-P12), although it disclosed less than AT&T and Telefónica. It clearly disclosed its process for responding to German government requests, but provided only limited information about how it responds to private requests and requests submitted by governments in foreign jurisdictions (P10). Like all of its peers, it failed to disclose anything about whether or not it notifies users of third-party requests to access their information (P12).

It also disclosed more about its security policies than the rest of its peers. It revealed that it monitors and limits employee access to user information and that it commissions third-party security audits (P13)—although it lacked clear disclosure about how it addresses security vulnerabilities (P14). It disclosed some information about its process for responding to data breaches (P15), but its disclosure was less comprehensive than that of Vodafone (P16).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/DTE:GR

Telecommunications company

Etisalat Group

Operating company evaluated:

- **Etisalat UAE (United Arab Emirates)**

Services evaluated:

- **Etisalat UAE (Prepaid mobile)**
- **Etisalat UAE (Postpaid mobile)**
- **Etisalat UAE (Fixed-line broadband)**

Rank	Score	Difference
11	8%	▼ 0.13

Rank among 12 telecommunications companies

Key findings

- Etisalat was the second-lowest scoring telecommunications company in the Index, disclosing almost nothing about policies and practices affecting users' freedom of expression and privacy.
- Etisalat did not publish a privacy policy, making it impossible for users to understand what the company does with their information, including what it collects and for what purposes.
- Etisalat disclosed nothing about how it handles government and private requests to hand over user information.

Key recommendations

- **Publish privacy policies:** Etisalat should clearly disclose how it handles user information and make its policies both easy to find and understand.
- **Be transparent about private requests:** Etisalat should disclose how it responds to private requests to block content or accounts and to hand over user data, and regularly publish data about the requests.
- **Improve redress:** Etisalat should improve its existing grievance mechanisms by explicitly including complaints related to freedom of expression and privacy, and by providing clear remedies for these types of complaints.

Analysis

Etisalat ranked eleventh out of the 12 telecommunications companies evaluated, disclosing almost nothing about its policies and practices affecting freedom of expression and privacy.[1] It made no improvements to its disclosure of policies evaluated by the RDR Index over the last year.[2] Etisalat is a majority state-owned company, operating in a political and regulatory environment that restricts expression online.[3] While companies in the UAE are discouraged from making public commitments to human rights, Etisalat could still be more transparent about basic policies affecting users' freedom of expression and privacy. The operating company Etisalat UAE did not publish a privacy policy, making it impossible for users to understand how the company handles their information.[4] Etisalat provided little information about its security policies, although there is no law prohibiting companies from being more transparent in this area. Given that the company is majority state-owned and that the overall operating environment discourages transparency, it is unlikely Etisalat would disclose information about government requests to block content or to hand over user information. However, it could disclose its policies for responding to private requests.

Etisalat Group operates telecommunications, fiber optics networks, and other services in the United Arab Emirates and across the Middle East, Africa, and Asia.

Market cap: USD 39.4 billion[5]
ADX: ETISALAT
Domicile: United Arab Emirates (UAE)
Website: https://www.etisalat.com/

Governance 3%

Etisalat performed poorly in the Governance category, scoring higher than only Ooredoo. It did not publish a commitment to respect users' freedom of expression and privacy as human rights (G1), and failed to disclose evidence of senior-level oversight over these issues at the company (G2). It also revealed no evidence of carrying out human rights due diligence, such as conducting risk assessments (G4), or of engaging with stakeholders on freedom of expression or privacy issues (G5). It received some credit for disclosing a grievance and remedy mechanism, though the company did not explicitly state that this process includes complaints related to freedom of expression or privacy (G6).

Freedom of Expression 15%

Etisalat disclosed little about its policies affecting freedom of expression. Etisalat UAE's terms of service policies were not easy to find, but were available in the primary languages of its home market and were presented in an understandable manner (F1). It disclosed some information about how its rules are enforced (F3) and how users are notified when the company takes actions to restrict accounts (F8).

However, aside from some minimal disclosure about reasons why it may restrict access to its network or specific applications and protocols due to government demands (F10), the company failed to disclose any other information about its policies or practices that affect users' freedom of expression. It failed to disclose any information about its network management policies or commit to uphold net neutrality principles (F9). Like many telecommunications companies, Etisalat provided no information about how it handles government or private requests to block content or restrict accounts (F5-F7). It did not publish any data on the number of such requests it received or with which it complied (F6, F7). Moreover, the company lost points due to a change in its disclosure, which made it less clear when it complies with private requests (F5). While it is a criminal offense in the UAE not to comply with government blocking orders, there is no law prohibiting Etisalat from disclosing how it handles these requests or its compliance rates with either government or private content-blocking requests.[6]

Privacy 4%

Etisalat received the second-lowest privacy score of all telecommunications companies evaluated, disclosing only slightly more than Qatar-based telecommunications operator Ooredoo. Like Ooredoo Qatar, Etisalat UAE did not publish a privacy policy, making it impossible for users to understand what the company does with their information, including what it collects, shares, and why. Aside from disclosing that it shares user information with government authorities if legally required and in cases of national security (P4), the company disclosed nothing about how it handles the user information it collects (P3-P8).

Etisalat provided no information about how it responds to third-party requests for user information, making it one of four companies, along with MTN, Ooredoo, and Axiata, that received no credit on these indicators (P10-P12). It provided no information about its process for responding to these types of requests (P10), or whether it notifies users when their information is requested (P12). However, Etisalat's operating license required it to install equipment allowing authorities to access the network, so the company may not be aware when government authorities access user information.[7] Still, there is no law specifically prohibiting Etisalat from disclosing its policy for responding to user information requests that come through private processes.

Etisalat UAE disclosed almost nothing about its security policies and practices, scoring better than only Ooredoo Qatar on these indicators (P13-P18). It disclosed that it has policies governing employee access to user data and has security teams monitoring for security threats and data breaches (P13). However, the company provided no additional information regarding its internal processes for ensuring that user data is secure, including whether it commissions external security audits (P13). It disclosed nothing about policies for addressing security vulnerabilities (P14) or for responding to data breaches (P15). There are no apparent legal obstacles to disclosing this information.

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index. For Etisalat's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/etisalat

[2] For Etisalat's performance in the 2018 Index: rankingdigitalrights.org/index2018/companies/etisalat/

[3] "Freedom on the Net" (Freedom House, November 2018), freedomhouse.org/report/freedom-net/2018/united-arab-emirates

[4] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Etisalat UAE

[5] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/ETISALAT:UH

[6] "Federal Decree-Law No. (5) of 2012 on Combating Cybercrimes" (2012), ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf

[7] "Public Telecommunications License No. 1/2006" Telecommunications Regulatory Authority, accessed March 15, 2018, www.tra.gov.ae/assets/03VgXUV3.pdf.aspx

Internet and mobile ecosystem companies

Facebook, Inc.

Services evaluated:

- **Facebook** [Social networking & blog]
- **Instagram** [Video & photo sharing]
- **Messenger** [Messaging & VoIP]
- **WhatsApp** [Messaging & VoIP]

Rank	Score	Difference
4	57%	^ 2.53

Rank among 12 internet and mobile ecosystem companies

Key findings

- Facebook lacked clarity about its handling of user information and about what it does to keep user data secure—including policies limiting employee access to user data and for handling data breaches.
- Facebook improved disclosure of how it enforces its own rules, but it disclosed less than in previous years about how it responds to government requests to remove content or deactivate accounts.
- While Facebook failed to disclose enough about its policies and practices affecting users' freedom of expression and privacy, its relatively high place in the ranking was due, in part, to greater transparency about policies related to government demands.

Key recommendations

- **Clarify handling of user information:** Facebook should disclose more about its handling of user information and its policies to keep user information secure.
- **Improve human rights due diligence:** Facebook should demonstrate it carries out human rights risk assessments on existing products and services, as well as on its terms of service enforcement, its use of automated decision-making, and its targeted advertising policies and practices.
- **Improve appeals mechanisms:** Facebook should improve its grievance and remedy mechanisms for users whose freedom of expression and privacy are violated by the company's policies and practices.

Analysis

Facebook ranked fourth out of the 12 internet and mobile ecosystem companies evaluated,[1] disclosing less about policies and practices affecting freedom of expression and privacy than Microsoft, Verizon Media,[2] and Google.[3] While it introduced a raft of policy changes over the last year in response to scrutiny by the public and lawmakers over its unclear content moderation policies[4] and its mishandling of user data, these changes still fell short in key areas.[5] Although Facebook improved its disclosure of actions it took to police content as a result of violations to its own rules, it disclosed less than in previous years about how it responds to third party requests to remove content or deactivate accounts. While it made numerous revisions to its privacy policy that clarified different aspects of how it handles user data, these steps still fell vastly short of giving users a clear picture of its data collection and sharing policies—or clear options to control what is being collected and shared. Facebook also lacked clarity about what it does to keep user data secure, including whether it monitors employee access to user data and its policies for handling data breaches. As in previous years, Facebook's grievance and remedy mechanisms remained among the weakest of any company in the RDR Index.

Facebook, Inc. operates social networking platforms for users globally.

Market cap: USD 510.5 billion[6]
NasdaqGS: FB
Domicile: USA
Website: https://www.facebook.com

Governance 78%

A member of the Global Network Initiative (GNI), Facebook received the third-best governance score among the 12 internet and mobile ecosystem companies evaluated, behind Microsoft and Verizon Media. While it published a clear commitment to respect and protect human rights to freedom of expression and privacy (G1), it disclosed little about its due diligence efforts aimed at ensuring that its business operations and practices actually protect these rights in practice (G4). For instance, it disclosed nothing about whether it conducts risk assessments around its targeted advertising policies and practices, or about its use of automated decision-making technologies (G4).

Facebook also had one of the lowest scores of any company in the Index for its appeals mechanisms—even after introducing improvements to its appeals process over the last year. In April 2018, Facebook (the social network) unveiled a new process for remedying wrongful takedowns, but it was not clear if the scope of this appeals mechanism includes any type of violation to its Community Standards.[7] Meanwhile, the company lacked a clear appeal mechanism for users to seek remedy when they feel that Facebook has violated their privacy.

Freedom of Expression 47%

Despite notable improvements, Facebook failed to disclose enough about its policies affecting freedom of expression, and scored below most of its U.S. peers in this category. It provided relatively clear information about its rules and what types of activity and content are prohibited on its services (F3): it received one of the top scores on this indicator, after Microsoft. While Facebook published its first ever Community Standards Enforcement Report in May 2018[8]—making it one of just four companies in the RDR Index to disclose data about the nature and volume of content it removed, or accounts it restricted for rules violations (F4)—this data applied just to Facebook (the social network) and not to Instagram, WhatsApp, or Messenger.

Facebook also disclosed significantly less than in previous years about its process for handling and complying with government requests to restrict content or accounts (F5-F7). Whereas its previous transparency reports specified that data about compliance with government requests applied to all services, Facebook's latest transparency report (January - June 2018) failed to state if the data included information about WhatsApp or Messenger (F5, F6). The company's overall score in the freedom of expression category declined this year as a result.

Privacy 55%

Facebook disclosed less about its privacy policies and practices than most of its U.S. peers, including Microsoft, Apple, Google, and Verizon Media. While it made numerous revisions to its privacy policies that clarified different aspects of how it handles user data, those revisions fell short of giving users a clear picture of its data collection and sharing policies—or of options for users to control what is being collected and shared. It remained among the least transparent of any internet and mobile ecosystem company about options users have to control how their data is used, including for the purposes of targeted advertising (P7). Facebook was also less transparent than Google, Apple, Microsoft, and Verizon Media about its policies for keeping user data secure (P13-P18): it revealed little about its policies for limiting employee access to user data (P13), and disclosed nothing about its policies for handling data breaches (P15).

In contrast, Facebook's clarifications about ways users can obtain their data (P8) earned it the top score on that indicator. Of the internet and mobile ecosystem companies evaluated, it was among the most transparent about its handling of government and other types of third-party requests for user information (P10-P12), and was one of the few companies to commit to notifying users of government requests for their data (P12). Like other U.S. companies, Facebook did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.[9] Facebook provided end-to-end encryption by default for WhatsApp, and gave Messenger users the option to enable end-to-end encryption, although it is not on by default. In contrast, it failed to disclose any information about its encryption practices for Instagram (P16).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] Oath, which provides a range of communications services including Yahoo Mail and Tumblr, updated its name to Verizon Media on January 7, 2019.

[3] For Facebook's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/facebook

[4] Julia Carrie Wong and Olivia Solon, "Facebook releases content moderation guidelines – rules long kept secret," Guardian, April 24, 2018. www.theguardian.com/technology/2018/apr/24/facebook-releases-content-moderation-guidelines-secret-rules

[5] Kieran Corcoran, "Facebook is overhauling its privacy settings in response to the Cambridge Analytica scandal," Business Insider, March 28, 2018, www.businessinsider.com/facebook-overhauls-privacy-settings-after-cambridge-analytica-scandal-2018-3

[6] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/FB:US

[7] "Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process," Facebook, April 24, 2018, newsroom.fb.com/news/2018/04/comprehensive-community-standards

[8] "Community Standards Enforcement Report," Facebook, transparency.facebook.com/community-standards-enforcement

[9] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Internet and mobile ecosystem companies

Google LLC

Services evaluated:

- **Google Search** [Search engine]
- **Gmail** [Email]
- **YouTube** [Video & photo sharing]
- **Android** [Mobile ecosystem]
- **Google Drive** [Cloud service]

Rank	Score	Difference
2	61%	^ 1.85

Rank among 12 internet and mobile ecosystem companies

Key findings

- Google disclosed more than all other internet and mobile ecosystem companies evaluated—apart from top-ranked Microsoft—about policies and practices affecting privacy and freedom of expression, but still fell short in key areas.
- The company continued to lag behind its peers for weak governance and oversight over its impact on human rights, including freedom of expression and privacy.
- Google was less transparent about its security policies than many of its peers, and failed to disclose anything about its policies for handling data breaches.

Key recommendations

- **Improve remedy:** Google should be more accountable to users by providing clear and accessible channels for users to communicate human rights grievances and obtain appropriate remedy.
- **Do more to protect privacy:** Google should clarify what information it collects and shares, and for what purpose—and give users clear options to control what data is collected and shared about them.
- **Clarify security practices:** Google should disclose more about its processes for keeping user information secure and how it responds to data breaches.

Analysis

Google tied with Verizon Media[1] for the second-highest score among internet and mobile ecosystem companies, behind Microsoft.[2] The company's ranking dropped from first to second place in this year's Index, due to the addition of the Google Drive cloud service to the evaluation, which had less clear disclosure and pulled down Google's overall score.[3] As a member of the Global Network Initiative (GNI), Google remained one of the stronger performers in the Index, disclosing more than most of its peers about policies and practices affecting freedom of expression and privacy. It was among a limited number of companies to improve its disclosure of policies affecting freedom of expression and, as in previous years, it was among the most transparent about how it handles government requests to remove content, deactivate accounts, or hand over user data. But there is ample room for improvement: Google failed to adequately disclose what user information it shares and also failed to give users clear options to control what data it collects and shares. It lacked transparency about what it does to keep user data secure, and provided no information whatsoever about its policies for responding to data breaches. It also failed to provide adequate redress mechanisms for users to communicate human rights grievances and obtain appropriate remedy.

Google LLC, a subsidiary of Alphabet Inc., is a global technology company with services that include Google Search, Gmail, YouTube, and Google Cloud. It also offers consumer hardware products and systems software, like its open-source mobile operating system, Android.

Market cap: USD 860.7 billion[4] (Alphabet Inc.)
NasdaqGS: GOOGL
Domicile: USA
Website: https://google.com

Governance 71%

For the third year in a row, Google continued to lag behind its peers in the Governance category, disclosing less about its governance and oversight over human rights issues than other members of GNI. While it made some progress by specifying that the board indeed has oversight over privacy issues at the company (G2)—which it had consistently failed to clarify since re-organizing under Alphabet in 2015—it remained opaque about governance of its freedom of expression and privacy commitments in other areas. Google stood out for its lack of clear and accessible channels for users to communicate human rights grievances and obtain appropriate remedy (G6). It failed to disclose if the scope of its risk assessments include evaluation of possible harms associated with enforcing its terms of service, its use of automated decision-making technologies, or its targeted advertising policies and practices (G4).

Freedom of Expression 61%

Google disclosed more than any of its peers about policies and practices affecting freedom of expression—it was among the few internet and mobile ecosystem companies to make improvements in this category—but still lacked transparency in key areas. The company's lead in this category was primarily due to stronger transparency about its handling of government requests to remove content or deactivate accounts (F5-F6): it disclosed more about its processes and compliance with these requests than any other company apart from Verizon Media. Google also had relatively strong disclosure of its rules and enforcement processes compared to its peers—only Microsoft's and Facebook's terms were more clear—and it clarified that YouTube gives government agencies special status when flagging content that violates YouTube's rules (F3). Google also improved disclosure of its commitment to notify users when it restricts Gmail accounts (F8).

Although it took important steps to improve, Google's transparency about the actions it took to enforce its own terms of service remained uneven (F4). In April 2018, YouTube released its first Community Guidelines Enforcement Report, which contained more comprehensive data about content the company removed for violating its rules (F4).[5] However, Google disclosed nothing about actions it took to enforce its rules for other services. It also disclosed almost no data about its compliance with private requests to remove content or disable accounts—revealing significantly less information than Verizon Media, Twitter, Kakao, Microsoft, and Facebook (F7).

Privacy 58%

Google tied with Apple for the second-best privacy score among internet and mobile ecosystem companies, after Microsoft. Its higher score in this category was a result of its strong disclosure of how it handles government requests for user information (P10, P11). Notably, Google made a clear commitment to challenge overbroad government requests, and provided clear examples and guidance of how it handles these types of requests (P10). Like other U.S. companies, Google did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.[6]

Google lacked transparency about its handling of user data—despite revealing more information than most of its peers. It gave some information about what user information it collects (P3) but revealed less about what data it shares (P4). It improved its disclosure of its retention periods for some types of user information, but failed to disclose how long it retains each type of information collected, or whether it deletes all user information after users terminate their account (P6). Google also lost points for its vague disclosure of whether Android mobile users have the ability to turn off location data: the company previously stated that Android users could control whether the company collected location data through a setting at the device level. However, Google's revised policy on managing location history stated that some location data may still be collected even when location history is turned off (P7).

Google was also less transparent about its security policies and practices, disclosing less than Apple, Microsoft, Kakao, and Yandex (P13-P18). While it earned the highest score for disclosing ways for users to keep their accounts secure (P17), it failed to disclose anything about its policies for handling data breaches (P15). Google disclosed that it encrypts user traffic by default, but did not provide an option for users to end-to-end encrypt their private content or communications for Gmail, YouTube, or Google Drive (P16).

Footnotes

[1] Verizon Media operates Yahoo Mail! and Tumblr. It was previously named Oath and was renamed Verizon Media on January 7, 2019.

[2] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[3] For Google's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/google

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/GOOGL:US

[5] YouTube Community Guidelines Enforcement Report, transparencyreport.google.com/youtube-policy/removals?hl=en

[6] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Internet and mobile ecosystem companies

Kakao Corp.

Services evaluated:

- **Daum Search [Search engine]**
- **Daum Mail [Email]**
- **KakaoTalk [Messaging & VoIP]**

Rank	Score	Difference
6	50%	^ 1.52

Rank among 12 internet and mobile ecosystem companies

Key findings

- Kakao failed to publish a strong commitment to respect users' freedom of expression and privacy rights, but disclosed more about its policies affecting freedom of expression than many of its peers.
- Kakao disclosed more than many of its peers about how it handles government requests to restrict content or accounts or hand over user information, but did not disclose information or data about government requests received from outside of South Korea.
- While Kakao improved its disclosure of how it handles data breaches, it disclosed little information about its handling of security vulnerabilities.

Key recommendations

- **Improve human rights policy commitment:** Kakao should commit to respect users' freedom of expression and privacy in accordance with international human rights standards.
- **Improve transparency around content and account restrictions:** Kakao should publish data on content and accounts it restricted to enforce its rules, and commit to notify users of these types of restrictions.
- **Be more transparent about handling of user information:** Kakao should improve its disclosure of whether and how it collects data by tracking users across the internet.

Analysis

Kakao ranked sixth out of the 12 internet and mobile ecosystem companies evaluated.[1] With an overall score of 50 percent, the company failed to disclose sufficient information about policies and practices affecting freedom of expression and privacy—although it was more transparent than its South Korean peer, Samsung. Kakao improved its disclosure of how it responds to data breaches but did not make any other improvements resulting in score changes in this year's Index.[2] South Korean law, such as requirements for grievance mechanisms and transparency around the collection and sharing of user information, helped boost the company's performance.[3] However, the company still fell short in key areas: for instance, it did not publish any data about content or accounts restricted to enforce its rules or a commitment to notify users of such restrictions, although there are no legal barriers preventing Kakao from disclosing such information.

Kakao Corp. provides online communication and search services in South Korea and internationally, with products that include web-based mail and messaging, a search engine, and maps and location services.

Market cap: USD 8.8 billion[4]
KOSDAQ: A035720
Domicile: South Korea
Website: https://www.kakaocorp.com

Governance 33%

Kakao received the sixth-highest score in the Governance category, slightly outperforming its South Korean peer, Samsung. The company made a commitment to protect users' privacy, although its commitment fell short of explicitly referring to international human rights standards, and it made no similar commitment with regards to freedom of expression (G1). It disclosed executive- and management-level oversight over privacy issues (G2) and that it trains employees on such issues (G3). While Kakao disclosed some information about assessing privacy impacts, it disclosed little else regarding its implementation of human rights impact assessments (G4), and, like most companies, disclosed no information on whether it assesses freedom of expression and privacy risks associated with its use of automated decision-making and its targeted advertising practices and policies. On a positive note, Kakao disclosed more about its grievance and remedy processes than any other internet and mobile ecosystem company evaluated (G6).[5] Companies are required by law to offer users an avenue for lodging grievances.[6]

Freedom of Expression 53%

Kakao disclosed more information about its policies affecting users' freedom of expression than Apple and Facebook, but there was ample room for improvement. Kakao published terms of service that were easy to locate and relatively easy to understand (F1) but did not clarify how it directly notifies users of changes (F2). Kakao revealed more about its policies for restricting content and accounts than many of its peers. It disclosed the types of content and activities it does not allow on its services (F3) and disclosed some information about its policy of notifying users of such restrictions (F8). However, like most companies, Kakao disclosed no data about the volume or types of service violations (F4).

Kakao disclosed more than Microsoft, Apple, and Facebook about its handling of government and private requests to remove content or restrict accounts (F5-F7). Kakao was more transparent about its process for responding to private requests than government requests (F5). Notably, the company did not provide data about government requests to restrict content or accounts from outside of South Korea (F6). It disclosed more data about private requests it received to block content or restrict user accounts (F7) than many of its peers, including Apple and Google.

Privacy 54%

Kakao disclosed substantially more than its South Korean peer Samsung about policies affecting users' privacy and security, but disclosed less than all of the U.S.-based internet and mobile ecosystem companies. Kakao's privacy policies were easy to find and understand, and disclosed a commitment to notify users of changes to these policies, though it was not always clear how users would be notified (P1, P2). Kakao clearly disclosed what types of user information it collects (P3) and disclosed the most about what user information it shares and with whom (P4). However, it was less transparent about its purposes for collecting and sharing user information (P5), and failed to disclose a time frame for deleting information when users terminate their accounts (P6). It provided users with some options to control the company's collection of their information and the right to opt out of targeted advertising (P7). It disclosed nothing about whether or how it tracks users across the internet (P9).

Kakao disclosed less about how it handles government and private requests for user information than all U.S. internet and mobile ecosystem companies evaluated, but more than the rest of its peers (P10, P11). It provided no information about whether it notifies users of government or private requests for user information (P12). Kakao offered more disclosure than Facebook and its South Korean counterpart Samsung about its security policies (P13-P18). It was the only company to fully disclose the internal measures it takes to secure users' information, including conducting security audits and limiting and monitoring employee access to user data (P13). It improved its transparency about how it addresses data breaches (P15). However, it provided insufficient information about measures taken to address security vulnerabilities (P14) and its encryption practices across different services (P16).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Kakao's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/kakao.

[3] 'Act on Promotion of Information and Communications Network Utilization and Information Protection (ICNA)', 22 March 2016; 'Telecommunications Business Act', 19 May 2011.

[4] Bloomberg Markets, Accessed April 18, 2019, https://www.bloomberg.com/quote/035720:KS

[5] South Korean law requires companies to offer a grievance mechanism. See: 'Act on Promotion of Information and Communications Network Utilization and Information Protection (ICNA)', 22 March 2016; 'Telecommunications Business Act', 19 May 2011.

[6] 'Act on Promotion of Information and Communications Network Utilization and Information Protection (ICNA)', 22 March 2016; 'Telecommunications Business Act', 19 May 2011.

Internet and mobile ecosystem companies

Mail.Ru Group Limited

Services evaluated:

- **Mail.Ru [Email]**
- **Mail.Ru Agent [Messaging & VoIP]**
- **VKontakte [Social networking & blog]**
- **Cloud [Cloud service]**

Rank	Score	Difference
12	21%	^ 0.08

Rank among 12 internet and mobile ecosystem companies

Key findings

- Mail.Ru earned the lowest score of all internet and mobile ecosystem companies in the Index, disclosing less about policies affecting users' freedom of expression and privacy than any of its peers, including Yandex, the other Russian internet company evaluated.
- Mail.Ru disclosed almost nothing about how it handles government demands to remove content or hand over user data, although there are no legal barriers to disclosing at least some information about its processes for responding to these types of requests.
- Mail.Ru lacked transparency about options users have to control and access their own information and the measures it takes to keep that information secure.

Key recommendations

- **Make a clear commitment to human rights:** Mail.Ru should make a clear commitment to respect freedom of expression and privacy as human rights, as there are no legal obstacles preventing it from doing so.
- **Be transparent about demands to block content or hand over user information:** Mail.Ru should disclose information on its process for handling government requests to remove content or hand over user information, and indicate where laws may complicate full transparency.
- **Clarify handling of user information:** Mail.Ru should improve disclosure of its handling of user data and communicate to users what steps it takes to keep that information secure.

Analysis

While Mail.Ru's overall score improved slightly in this year's Index,[1] it earned the lowest score of all 12 internet and mobile ecosystem companies evaluated, disclosing the least about policies affecting freedom of expression and privacy than all other internet and mobile ecosystem companies evaluated.[2] It disclosed significantly less than Yandex, the other Russian company evaluated, about its governance and oversight over freedom of expression and privacy issues at the company. It disclosed very little about how it handles government demands to remove content or hand over user data, and lacked transparency about options users have to control and access their own information. It also disclosed little about the measures it takes to keep that information secure. While operating in an increasingly restrictive internet environment, it could be more transparent about key policies and practices affecting freedom of expression and privacy, such as its content moderation policies, how it handles user information, and how it keeps that information secure.[3]

Mail.Ru Group Limited provides online communication products and entertainment services in Russia and internationally. Services include a search engine, social networking platforms, email services, and gaming and e-commerce platforms.

Market cap: USD 5.4 billion[4]
LSE: MAIL
Domicile: Russia
Website: https://corp.mail.ru

Governance 6%

Mail.Ru disclosed almost nothing about its governance and oversight over human rights issues at the company, and received the second-lowest score among internet and mobile ecosystem companies in this category. It did not publish a formal commitment to respect users' freedom of expression and privacy (G1)—although the other Russian company evaluated, Yandex, did publish such a commitment, demonstrating that such disclosure is possible. It disclosed some information about a whistleblower program for employees to raise concerns about violations of its code of conduct, though it was not clear if the scope included human rights concerns (G3), and it provided a grievance mechanism for users to issue complaints related to freedom of expression and privacy issues, but failed to disclose comprehensive information about its process or time frame for providing remedy to these complaints (G6).

Freedom of Expression 24%

Mail.Ru disclosed little about policies affecting users' freedom of expression, though it did disclose more than the other Russian company evaluated, Yandex. Mail.Ru's terms for its services were not always easy to understand (F1), and it did not clearly disclose whether it provides notice to users when it changes its terms for all services evaluated (F2). It clearly disclosed its rules, but not its process for enforcing them (F3), and, like most companies in the Index, it disclosed no data about the volume and nature of content or accounts it restricted for terms of service violations (F4). Unlike Yandex, Mail.Ru did not disclose any information about whether it notifies users when it restricts their content or accounts (F8).

Mail.Ru disclosed almost nothing about its process for handling government and private requests to restrict content or accounts (F5-F7). It provided only minimal information about its processes for responding to these types of requests (F5), and offered no data about the number of requests it receives or complies with (F6, F7), although there are no laws prohibiting Mail.Ru from doing so.

Privacy 24%

Mail.Ru received the lowest privacy score of the 12 internet and mobile ecosystem companies evaluated. It was one of three internet and mobile ecosystem companies that failed to disclose any information about its processes for handling government and private requests for user information (P10, P11). Like many of its peers, it also disclosed nothing about whether it notifies users when their data has been requested (P12). However, since Russian authorities may have direct access to communications data, Russian companies may not be aware of when government authorities access user information.[5]

Mail.Ru disclosed less than all other internet and mobile ecosystem companies, including Yandex, about how it handles user information (P3-P9). It did not disclose anything about what user data it shares and with whom, aside from acknowledging that it may share user data with government authorities (P4). While it improved its disclosure of the purposes for which VKontakte collects user information (P5), a commitment previously disclosed by Mail.Ru to limit VKontakte's use of user information for the purposes for which it is collected was no longer available (P5). On the plus side, VKontakte's privacy policy was more transparent about how it collects user information from third-party websites using cookies (P9).

Mail.Ru disclosed less than most of its peers, including Yandex, about its policies for keeping user information secure (P13-P18). It failed to disclose if it limits and monitors employee access to user information (P13). It did, however, disclose that it has a mechanism for researchers to report security vulnerabilities (P14). Like most companies, it offered no information about its process for responding to data breaches (P15). It also disclosed little about its encryption policies, particularly in comparison to Yandex, the other Russian internet company evaluated, which received the second-highest score on this indicator (P16).

Footnotes

[1] For Mail.Ru's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/mailru

[2] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[3] "Freedom on the Net" (Freedom House, November 2018), freedomhouse.org/report/freedom-net/2018/russia

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/MAIL:LI

[5] Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," The Guardian, September 8, 2015, www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet

Internet and mobile ecosystem companies

Microsoft Corp.

Services evaluated:

- **Bing** [Search engine]
- **Outlook.com** [Email]
- **Skype** [Messaging & VoIP]
- **OneDrive** [Cloud service]

Rank	Score	Difference
1	62%	^ 1.26

Rank among 12 internet and mobile ecosystem companies

Key findings

- Microsoft earned the top score among internet and mobile ecosystem companies in the 2019 Index for disclosing more about its commitments and policies affecting users' human rights than all other ranked companies.
- It was the most transparent of all internet and mobile ecosystem companies about its privacy policies and practices, although it disclosed less than some of its peers about how it handles user data.
- It was less transparent than many of its peers about policies affecting freedom of expression, including how it handles third-party requests to remove content or restrict accounts, as well as its policies for notifying users of such restrictions.

Key recommendations

- **Be more transparent about handling of user information:** Microsoft should more clearly state what user information it collects, shares, retains, and why, and clarify options users have to control what is collected and shared, and how.
- **Be transparent about restrictions to freedom of expression:** Microsoft should clarify how it notifies users when it restricts access to content or accounts either due to government requests or as a result of enforcing its own rules.
- **Improve remedy:** Microsoft should be more accountable to users by providing a clear and accessible remedy mechanism for users to issue human rights grievances against the company.

Analysis

Microsoft was the highest scoring internet and mobile ecosystem company in the 2019 Index, disclosing more information about policies and practices affecting users' freedom of expression and privacy than its peers.[1] It earned the top score in this year's Index for its improved disclosure of privacy and security policies.[2] It disclosed more information about options users have to access the information that the company holds about them, clarified its process for responding to data breaches, and disclosed options users have to use end-to-end encryption for some of its services. Despite its strong overall performance relative to its peers, Microsoft should be more transparent about its policies affecting users' freedom of expression by clarifying its rules and how they are enforced. It could also improve its disclosure of its handling of user information.

Microsoft Corp. develops, licenses, and supports software products, services, and devices worldwide. Major offerings include Windows OS, Microsoft Office, Windows Phone software and devices, advertising services, server products, Skype, and OneDrive cloud services.

Market cap: USD 934.2 billion[3]
NasdaqGS: MSFT
Domicile: USA
Website: https://www.microsoft.com

Governance 85%

Microsoft received the highest score in the Governance category among internet and mobile ecosystem companies, and the second-highest score of all 24 companies evaluated, after Telefónica. A member of the Global Network Initiative (GNI), Microsoft continued to disclose strong governance oversight over freedom of expression and privacy issues, including clear evidence that it conducts human rights due diligence to assess and mitigate the risks of its products and services (G4). It was one of the few companies in the 2019 Index to disclose it evaluates freedom of expression and privacy risks associated with how it enforces its terms of service and its use of automated decision making technologies. However, it failed to disclose if it evaluates risks of its use of targeted advertising on freedom of expression and privacy. Like all companies, Microsoft should do more to clarify its grievance and remedy mechanisms enabling users to submit complaints about infringements to their freedom of expression or privacy rights (G6).

Freedom of Expression 55%

Though it made some improvements, Microsoft's weakest performance in this year's Index was in the Freedom of Expression category, ranking fourth among its internet and mobile ecosystem company peers. Microsoft's terms of service were easy to find and easy to understand (F1). It clarified its policy for notifying users of changes to its terms of service for the Bing search engine, but failed to disclose a notification time frame for any of its services (F2).

Microsoft disclosed less than Twitter, Google, and Kakao but more than all other internet and mobile ecosystem companies about its rules and how they are enforced (F3, F4, F8). Microsoft disclosed the most information about its process for enforcing its rules (F3), but failed to disclose clear policies for notifying users of content or account restrictions (F8). Microsoft was one of four companies to publish any data about its terms of service enforcement (F4), specifically on content removed from Bing and OneDrive for violating its policy on "non-consensual pornography." However, it should disclose data on other types of content it removes for terms of service violations.

Microsoft provided less information than Google, Verizon Media, Kakao, and Twitter about how it responds to government and private requests to remove content or restrict accounts (F5-F7).[4] It disclosed some information about the company's process for responding to government and private requests to remove content (F5), and some data about the number of these requests received and with which it complied (F6, F7).

Privacy 59%

Microsoft received the highest score in the Privacy category among internet and mobile ecosystem companies for strong disclosure of its handling of government requests for user information, and of its security policies. But Microsoft disclosed less than Twitter, Google, Verizon Media, Facebook, and Apple about how it handles user information (P3-P9)—despite making some improvements over the last year. It did not fully disclose how it collects user information (P3), what information it shares (P4), or why (P5). Like most companies, it provided even less information about its data retention policies (P6). It also disclosed some options allowing users to control what data is collected for targeted advertising—which suggests that targeted advertising is on by default (P7).

Microsoft disclosed more than its peers about its process for handling government and private requests for user information (P10), but lagged behind Apple, Twitter, Facebook, and Google on disclosure of data on the requests it received (P11). Like other U.S. companies, it did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.[5] Microsoft disclosed its policy for notifying users about government requests for user information, but not for requests it receives through private processes (P12).

After Apple, Microsoft disclosed the most about its security policies than any other internet and mobile ecosystem company evaluated (P13-P18). Microsoft disclosed it conducts internal security audits (P13), and offered a bug bounty program to address security vulnerabilities (P14). It improved disclosure of its data breach notification policies for Outlook (P15). It also improved its disclosure regarding the availability of end-to-end encryption for both Outlook and Skype (P16).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Microsoft's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/microsoft

[3] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/MSFT:US

[4] Oath, which provides a range of communications services including Yahoo Mail and Tumblr, updated its name to Verizon Media on January 7, 2019. See: www.oath.com/2019/01/07/oath-is-now-verizon-media/

[5] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Telecommunications company

MTN Group Limited

Operating company evaluated:

- **MTN South Africa**

Services evaluated:

- **MTN South Africa [Prepaid mobile]**
- **MTN South Africa [Postpaid mobile]**
- **MTN South Africa [Fixed line broadband]**

Rank	Score	Difference
8	16%	^ 1.35

Rank among 12 telecommunications companies

Key findings

- MTN failed to disclose enough about policies and practices affecting users' freedom of expression and privacy.
- It lacked strong governance and oversight over human rights issues, and disclosed almost nothing about policies affecting freedom of expression.
- MTN disclosed very little about how it handles user information, particularly its policies around sharing and retaining user information, as well as what steps it takes to keep user information secure.

Key recommendations

- **Improve disclosure of human rights due diligence:** MTN should disclose more information about its human rights due diligence, including whether it conducts risk assessments on new and existing services and when entering new markets.
- **Be more transparent about handling of user information:** MTN should be explicit about what user information it collects and shares, for what purposes, and for how long it retains it.
- **Be more transparent about external requests affecting user rights:** MTN should disclose information about government and private requests to restrict access to content or accounts, and about private requests for user information.

Analysis

MTN ranked eighth out of the 12 telecommunications companies evaluated, tying with Bharti Airtel.[1] Despite making several improvements to its disclosure, MTN still lagged behind its peers, disclosing very little about policies and practices affecting freedom of expression and privacy.[2] It provided minimal information about how it responds to government demands to shut down its networks, and disclosed nothing about how it handles government requests to hand over user information. While South African law may discourage MTN from disclosing information about such requests, the company could still improve its disclosures in several other key areas. For instance, it could be more transparent about how it handles user information and its network management policies. It could also disclose more about its process for handling requests to block content or restrict user accounts.

MTN Group Limited is a telecommunications company that serves markets in 24 countries in Africa and the Middle East.[3] It offers voice and data services and business services, such as cloud, infrastructure, network, software, and enterprise mobility.

Market cap: USD 13.8 billion[4]
JSE: MTN
Domicile: South Africa
Website: https://www.mtn.com

Governance 39%

MTN disclosed weak governance and oversight over human rights issues. While it made some improvement by clarifying senior-level oversight over freedom of expression and privacy issues (G2), it fell short on most other indicators in this category. It published very limited information about conducting human rights impact assessments, failing to disclose whether it assesses freedom of expression and privacy related risks associated with its use of automated decision-making or its targeted advertising practices (G4). It had grievance and remedy mechanisms for users to submit their freedom of expression and privacy related complaints, but did not disclose its remedy procedures or specify a time frame for redressing these complaints (G6).

Freedom of Expression 9%

MTN disclosed almost nothing about policies and practices affecting freedom of expression, tying with Bharti Airtel for the lowest score of all telecommunications companies in this category. It provided no information at all about how it handles external requests to block content or deactivate accounts—it disclosed nothing about its process for handling government and private requests to block content or restrict user accounts (F5-F7). South African law does not prevent companies from disclosing information about how they handle these requests, nor does it prohibit them from publishing this data.

It also lacked transparency about its own internal processes for enforcing its rules: The terms for MTN South Africa's mobile and broadband services were not easy to find or understand (F1), and the company did not commit to notifying users of changes to these services (F2).[5] In addition, the operator revealed nothing about its network management policies and did not publish a clear commitment to uphold net neutrality (F9). Although it clarified reasons why it may shut down its networks, MTN still did not sufficiently disclose its policies for handling government network shutdown orders (F10).

Privacy 12%

MTN failed to disclose sufficient information about policies and practices affecting the privacy and security of its users, ranking tenth out of the 12 telecommunications companies in this category, ahead of only Etisalat and Ooredoo. MTN South Africa provided minimal information about the types of user information it collects and why (P3, P5), and no information about what information it shares (P4), or for how long it retains user information (P6). It also did not disclose any options for users to control what information the company collects and uses (P7), or options for users to obtain all of the information the company holds on them (P8).

MTN failed to provide any information about how it handles third-party requests for user information (P10-P12). The only piece of information MTN had previously disclosed was a commitment to push back on inappropriate or overbroad government requests; however, researchers were unable to locate such information in current company disclosures. While regulations in South Africa may discourage companies from publishing information about government requests for user information, including the fact that a request was made, nothing prevents MTN from fully disclosing how it handles private requests and the number of these requests it received and with which it complied.

The operating company MTN South Africa disclosed minimal information about its security policies, outperforming only Celcom (Axiata), Etisalat UAE, and Ooredoo Qatar on this set of indicators (P13-P18). It disclosed less than nearly all of its peers about its internal mechanisms to keep user information secure (P13)—but was one of only five telecommunications companies evaluated to disclose anything about its processes for addressing security vulnerabilities (P14). Like many of its peers, MTN South Africa provided no information about its policies for responding to data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For MTN's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/mtn

[3] "Where We Are," MTN Group, Accessed January 15, 2019, www.mtn.com/en/mtn-group/about-us/our-story/Pages/where-we-are.aspx

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/MTN:SJ

[5] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case MTN South Africa.

Telecommunications company

Ooredoo Q.S.C.

Operating company evaluated:

- **Ooredoo Qatar**

Services evaluated:

- **Ooredoo Qatar [Prepaid mobile]**
- **Ooredoo Qatar [Postpaid mobile]**
- **Ooredoo Qatar [Fixed-line broadband]**

Rank	Score	Difference
12	5%	▼ 0.26

Rank among 12 telecommunications companies

Key findings

- Ooredoo was the lowest scoring telecommunications company in the Index, disclosing almost nothing about its policies and practices affecting freedom of expression and privacy.
- Ooredoo revealed nothing about how it responds to government and other types of third-party requests to block or filter content, or government demands to shut down its networks.
- Ooredoo did not publish a privacy policy, making it impossible for users to understand what the company does with their information, including what it collects, shares, and why.

Key recommendations

- **Publish privacy policy:** Ooredoo should publish a privacy policy that is easy for its users to find and understand.
- **Clarify content and access restrictions:** Ooredoo should be more transparent about how it handles government and private requests to block content or restrict user accounts, and government requests to shut down networks.
- **Improve redress:** Ooredoo should clarify if its process for receiving complaints includes those related to freedom of expression and privacy, and provide clear remedies for these types of complaints.

Analysis

Ooredoo received the lowest score of all telecommunications companies, disclosing less about policies and practices affecting users' freedom of expression and privacy than any of its peers, including Etisalat, the UAE-based telecommunications company.[1] Ooredoo, which is majority owned by the government of Qatar, was one of three companies in the Index to make no improvements to its disclosure over the past year.[2] While the political and regulatory environment in Qatar discourages companies from making public commitments to human rights, Ooredoo could still be more transparent about basic policies affecting freedom of expression and privacy in a number of areas.[3]

Ooredoo Q.S.C. provides telecommunications services such as mobile, broadband, and fiber in Qatar and 11 other countries in the Middle East, North Africa, and Asia.[4]

Market cap: USD 5.2 billion[5]
DSM: ORDS
Domicile: Qatar
Website: https://www.ooredoo.qa

Governance 0%

Ooredoo received no credit on any indicator in this category, and disclosed nothing about its governance and oversight over human rights issues at the company. It did not make a public commitment to respect freedom of expression and privacy in line with international human rights principles (G1), nor did it disclose having senior-level oversight over these issues within the company (G2). Although it disclosed a whistleblower policy, it did not specify if it pertains to freedom of expression or privacy issues (G3). It offered no evidence that it has human rights due diligence processes in place (G4), or if it engages with stakeholders on freedom of expression or privacy issues (G5). Ooredoo Qatar did not offer a grievance mechanism for users to submit freedom of expression and privacy-related complaints, and there was no additional information about how it receives and responds to such grievances (G6).

Freedom of Expression 13%

Ooredoo disclosed minimal information about its policies affecting freedom of expression and tied with Axiata for the second-lowest score among telecommunications companies, ahead of MTN and Bharti Airtel. Ooredoo Qatar offered terms of service that were easy to find and understand (F1), and those terms gave some information about its rules and how they are enforced (F3).[6] It also disclosed some information about why it may need to shut down or restrict access to its networks (F10), though it did not disclose any other information about how it handles government demands to shut down its networks.

Ooredoo otherwise earned no credit on any of the other indicators in this category. Ooredoo Qatar failed to disclose any information about its network management policies (F9). The company also provided no information about its process for responding to government or private requests to block content or restrict users' accounts (F5), nor did it supply any data about the number of government or private requests to restrict content or accounts that it received or with which it complied (F6, F7). There is no apparent legal barrier to supplying this information. The lack of disclosure is likely a result of Ooredoo being majority state-owned as well as due to a general lack of transparency in the Qatari legal environment. Telecommunications companies in Qatar are legally required to comply with all judicial orders to block content, though there is no law prohibiting Ooredoo from disclosing its processes for handling these requests or its compliance rates with either government or private content-blocking requests.[7]

Privacy 0%

Ooredoo received the lowest privacy score of all companies evaluated. Ooredoo Qatar did not publish a privacy policy for any of its services, making it impossible for users to understand what the company does with their information, including what it collects, shares, and why (P1-P8). Ooredoo Qatar was also the only company to disclose nothing about its policies for keeping users' information secure (P13-P18). It did not disclose whether it has systems in place to monitor or limit employee access to user information (P13), nor did it provide any information about its processes for addressing security vulnerabilities or for handling data breaches (P14, P15).

Ooredoo provided no information about how it handles government or private requests for user information, making it one of four companies, alongside MTN, Etisalat, and Axiata, that received no credit on these indicators (P10, P11, P12). It provided no information about its process for responding to these types of requests (P10), or whether it notifies users when their information is requested (P12). Ooredoo also failed to publish any data on the number of requests it received for user information (P11). The lack of disclosure is likely a result of Ooredoo being majority state-owned as well as from a general lack of transparency in the Qatari legal environment. Still, there is no law specifically prohibiting Ooredoo from disclosing its policies for responding to user information requests that come through private processes.

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Ooredoo's performance in the 2018 Index: https://rankingdigitalrights.org/index2018/companies/ooredoo/.

[3] "Qatar 2017/2018," Amnesty International Report, 2018, www.amnesty.org/en/countries/middle-east-and-north-africa/qatar/report-qatar.

[4] "Our Markets," Ooredoo Corporate, Accessed January 15, 2019, ooredoo.com/en/who_we_are/our_markets

[5] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/ORDS:UH

[6] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Ooredoo Qatar.

[7] Peter Kovessy, "Qatar's Emir Signs New Cybercrime Legislation into Law," Doha News, September 16, 2014, dohanews.co/qatars-emir-signs-law-new-cybercrime-legislation/

Telecommunications company

Orange S.A.

Operating company evaluated:

- **Orange France**

Services evaluated:

- **Orange France [Prepaid mobile]**
- **Orange France [Postpaid mobile]**
- **Orange France [Fixed-line broadband]**

Rank	Score	Difference
6	36%	^ 1.72

Rank among 12 telecommunications companies

Key findings

- Orange disclosed strong governance and oversight over human rights issues, but failed to disclose adequate information about policies and practices affecting freedom of expression and privacy.
- Orange lacked transparency about how it handles government demands to hand over user data, to block or filter content, or to deactivate user accounts.
- It improved disclosure of how it handles user information, but disclosed less than its European peers about its security policies, including how it addresses vulnerabilities and responds to data breaches.

Key recommendations

- **Be transparent about government demands:** Orange should clearly disclose how it handles government demands for user data or to block or filter content and deactivate user accounts. It should publish the data about its compliance with these requests in all markets in which it operates.
- **Give users more control over their information:** Orange should let its users know what options they have to control their own information, including what information is collected, and how it is used for targeted advertising.
- **Improve security disclosures:** Orange should clarify what it does to protect user data and how it responds to data breaches.

Analysis

Orange ranked sixth among the 12 telecommunications companies evaluated, falling behind all of its European peers and AT&T.[1] A member of the Global Network Initiative (GNI) Orange stood out for its strong governance and oversight over its human rights commitments across its global operations. But the company lacked sufficient disclosure of policies and practices affecting users' freedom of expression and privacy.[2] Orange was especially opaque about how it deals with government requests to block or filter content or to hand over user data: the company's lack of transparency about government demands puts it out of step with its European counterparts. On the privacy side, Orange was more transparent, although there is ample room for improvement. Orange France did improve its clarity around its handling of user data in a number of areas. But it lacked disclosure of its policies for keeping user data secure, including its policies for responding to data breaches.

Orange S.A. provides telephone and mobile telecommunications and other services in Europe, Africa, and worldwide.

Market cap: USD 43.8 billion[3]
ENXTPA: ORA
Domicile: France
Website: https://www.orange.com

Governance 82%

Orange received the second-highest score among telecommunications companies in the Governance category, after Telefónica. A 2017 law in France requiring a "duty of vigilance" for multinationals means that strong human rights oversight and risk assessment are mandatory for Orange.[4] The company improved disclosure of its due diligence practices, clarifying that it systematically considers how laws in the different jurisdictions where it operates affect freedom of expression and privacy and that the company's board of directors considers the results of assessments and due diligence in their decision-making (G4). However, the company did not disclose whether it assesses risks associated with its use of automated decision-making or targeted advertising. Despite its strong disclosure across all indicators in this category, Orange could clarify its grievance and remedy procedures (G6): while it provided ways for users to appeal to the company if they feel their freedom of expression or privacy has been violated by the company, it offered less clear evidence that it is providing remedy to these complaints.

Freedom of Expression 17%

Orange disclosed less than all of its European peers, except Deutsche Telekom, about policies and practices affecting users' freedom of expression. The terms of service for Orange France's mobile and broadband services were easily accessible, but not easy to understand (F1), and did not clearly indicate a policy of notifying users when these terms change (F2).[5] Orange disclosed no information about how it handles government and private requests to block content or restrict user accounts (F5-F7)—although there are no legal obstacles in France preventing Orange from disclosing this information.

Orange France disclosed nothing about its network management practices (F9), making it one of five companies, along with Deutsche Telekom, Etisalat UAE, MTN South Africa, and Ooredoo Qatar, to receive no credit on this indicator (F9). While Orange provided an example of pushing back on government requests to shut down networks, it still revealed little about its processes for responding to these requests, lagging behind Telefónica, Telenor, and Vodafone (F10).

Privacy 31%

Despite some improvements, Orange still failed to disclose sufficient information about policies and practices affecting the privacy and security of its users—disclosing less overall across indicators in this category than all of its European peers and AT&T. The privacy policy covering Orange France's mobile and broadband services was easy to find and understand (P1), but did not specify if users are notified of policy changes (P2). It clarified the different types of user information it collects (P3), and provided some information about the purposes for collecting and sharing user data (P5). However, it failed to disclose if it shares data across company services (P5), disclosed very little information about what data is shared (P4) and did not give users clear options to control what information is collected and shared, including for the purposes of targeted advertising (P7).

Orange disclosed far less than its European peers and AT&T about how it handles government and private demands for user data (P10, P11). It revealed the legal basis for complying with the French government's requests, but gave no information about how it responds to these requests or those submitted by foreign governments (P10). It published some data about its compliance with government requests in France but not about those in other countries in which it operates (P11). If there are laws barring Orange from publishing this data, it should specify them. Like all the other telecommunications companies, Orange did not disclose if it notifies users about government requests for their data (P12).

Orange France also disclosed less than its European peers, AT&T, and América Móvil's Telcel about its security policies (P13-P18). It offered some information about its internal mechanisms to keep user information secure (P13), but revealed nothing about what it does to address security vulnerabilities (P14), or about it processes for responding to data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Orange's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/orange/

[3] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/ORA:FP

[4] "The French Duty of Vigilance Law: What You Need to Know," Corporate Social Responsibility and the Law, Foley & Hoag, www.csrandthelaw.com/2017/08/03/the-french-duty-of-vigilance-law-what-you-need-to-know/

[5] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Orange France.

Internet and mobile ecosystem companies

Samsung Electronics Co., Ltd.

Services evaluated:

- **Samsung's implementation of Android [Mobile ecosystem]**
- **Samsung Cloud [Cloud service]**

Rank	Score	Difference
9	29%	▼ 0.17

Rank among 12 internet and mobile ecosystem companies

Key findings

- Samsung disclosed less than most of its peers about its policies that affect users' freedom of expression and privacy, and scored below its South Korean peer, Kakao.
- Samsung received the second-lowest score of all internet and mobile ecosystem companies in the Privacy category, and disclosed less about its security policies than all of its peers.
- Samsung failed to provide any information about grievance and remedy mechanisms for freedom of expression and privacy complaints, although in South Korea companies are required to offer these mechanisms by law.

Key recommendations

- **Improve security disclosures:** Samsung should be more transparent about measures it takes to keep user information secure, including policies for responding to data breaches, and if it encrypts user communication and private content.
- **Offer remedy:** Samsung should provide users with grievance and remedy mechanisms to address their freedom of expression and privacy concerns.
- **Be transparent about third-party requests:** Samsung should publish data about third-party requests for content and account restrictions, and for user data.

Analysis

Samsung ranked ninth out of the 12 internet and mobile ecosystem companies evaluated, disclosing less than most of its peers about policies affecting users' freedom of expression and privacy.[1] It continued to lag behind Kakao, the other South Korean company evaluated in the Index. Samsung's overall score declined due to the company's less clear disclosure about its security policies.[2] It disclosed less information about how it addresses security vulnerabilities, and no longer provided users with information about how to defend themselves against cyber-risks. While South Korea has a strong data protection regime—for instance, it requires companies to obtain consent from users when collecting and sharing their information—Samsung still lacked clarity about these policies and practices in its public disclosures.[3] Companies are also legally required to offer grievance mechanisms, but Samsung did not publicly disclose clear options for users to submit freedom of expression and privacy-related complaints.

Samsung Electronics Co., Ltd. sells a range of consumer electronics, home appliances, and information technology solutions worldwide. Its products include televisions, mobile phones, network equipment, and audio and video equipment.

Market cap: USD 247.1 billion[4]
KOSE: A005930
Domicile: South Korea
Website: https://www.samsung.com

Governance 32%

Samsung disclosed less about its governance and oversight over human rights issues han most internet and mobile ecosystem companies, and slightly less than its South Korean counterpart Kakao. Samsung made a public commitment to respect users' human rights to freedom of expression and privacy (G1), but lacked clear evidence of how it ensures it is implementing these commitments across its global operations. It disclosed evidence of senior-level oversight over privacy issues, but not those pertaining to freedom of expression (G2). The company provided very little information about conducting human rights impact assessments, and, like most companies, failed to disclose whether it assesses risks associated with its use of automated decision-making and its targeted advertising practices and policies (G4). It did not disclose a commitment to engage with stakeholders on freedom of expression and privacy issues (G5) nor did it provide clear mechanisms for users to submit freedom of expression and privacy-related grievances (G6). Companies in South Korea are required by law to provide a complaints mechanism.[5]

Freedom of Expression 30%

Samsung disclosed little about its policies affecting users' freedom of expression, ranking eighth out of 12 internet and mobile ecosystem companies in this category. Samsung published terms of service that were easy to find and understand for Cloud, but not for Android (F1). However, while Samsung disclosed some information about why it may restrict access to content or accounts (F3), it disclosed no data about the volume or nature of content or accounts it restricted for violating these rules (F4). It revealed very little information about its policies for notifying users of content and account restrictions (F8), disclosing only a commitment to notify users and developers of Galaxy apps before terminating their access to the service.

Samsung was one of two internet and mobile ecosystem companies, including Chinese company Baidu, to disclose no information about its process for handling government or private requests to restrict content or user accounts (F5), or data about the number of such requests it received and with which it complied (F6, F7). There are no regulatory obstacles in South Korea preventing the company from disclosing this information. Notably, Kakao is far more transparent about these processes, demonstrating that increased disclosure of how the company handles these types of demands is possible.

Privacy 27%

Samsung received the second-lowest score of all internet and mobile ecosystem companies in the Privacy category, and disclosed less about its security policies than all of its peers. It was especially opaque about its handling of government and other types of third-party demands for user data—it was one of three internet and mobile ecosystem companies, including Tencent and Mail.Ru, to disclose nothing about its policies for handling these types of requests (P10) or data about the number of such requests it received and with which it complied (P11).

The company did not reveal enough about how it handles user data: it disclosed some information about the types of user information Samsung collects (P3), shares (P4), and for what purposes (P5), but was far less transparent about its policies for retaining user information (P6). While it provided users with some options to control their own information, including for purposes of targeted advertising (P7), it did not provide them with any options to access and obtain that information (P8).

Samsung also disclosed minimal information about its policies to keep user information secure (P13-P18). It disclosed that it monitors and limits employee access to user information and that it conducts data security audits, but failed to disclose whether it has a dedicated security team and if it commissions third-party security audits (P13). It disclosed some information about how it addresses security vulnerabilities, but was less clear about whether it made any modifications to the Android mobile operating system and how changes might impact users' ability to receive security updates (P14). It disclosed nothing about its policies for responding to data breaches (P15), or about what types of encryption are in place to protect user information in transit or on Samsung devices (P16).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Samsung performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/samsung

[3] 'Act on Promotion of Information and Communications Network Utilization and Information Protection (ICNA)', 22 March 2016. www.law.go.kr/법령/정보통신망이용촉진및정보보호등에관한법률;
'Personal Information Protection Act ("PIPA")', 29 March 2016. www.law.go.kr/법령/개인정보보호법

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/005930:KS

[5] 'Act on Promotion of Information and Communications Network Utilization and Information Protection (ICNA)', 22 March 2016. www.law.go.kr/법령/정보통신망이용촉진및정보보호등에관한법률 ; 'Telecommunications Business Act', 19 May 2011. www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95

Telecommunications company

Telefónica, S.A.

Operating company evaluated:

- **Telefónica Spain**

Services evaluated:

- **Movistar [Prepaid mobile]**
- **Movistar [Postpaid mobile]**
- **Movistar [Fixed-line broadband]**

Rank	Score	Difference
1	57%	^ 16.19

Rank among 12 telecommunications companies

Key findings

- Telefónica received the top score among telecommunications companies, and made the most improvements to its disclosure of policies affecting freedom of expression and privacy of any company evaluated.
- Telefónica disclosed more than all other companies about its governance and oversight over human rights issues, and was one of only three companies to disclose that it conducts human rights risk assessments on its use of automated decision-making technologies.
- Telefónica disclosed more than any telecommunications company about policies affecting freedom of expression, but still failed to disclose enough about how it handles government requests to block content and restrict user accounts.

Key recommendations

- **Clarify security policies:** Telefónica should be more transparent about its security policies, including how it responds to data breaches and how it addresses security vulnerabilities.
- **Clarify handling of user information:** Telefónica should disclose more about its handling of user information, including its data retention policies and practices.
- **Disclose more about third-party requests:** Telefónica should disclose more comprehensive data about how it responds to government and private requests to restrict access to content or accounts and to hand over user data.

Analysis

Telefónica received the highest score among telecommunications companies in the 2019 RDR Index, disclosing more about its commitments, policies, and practices affecting freedom of expression and privacy than any of its peers.[1] It made the most improvements of any company evaluated this year, topping Vodafone for the number one spot in this year's ranking.[2] It improved its disclosure of policies affecting users' freedom of expression and privacy, including how it handles government requests to restrict content and accounts, to shut down its networks, and to hand over user data. Still, there is room for improvement. Telefónica should publish data about actions it takes to restrict content and accounts that violate its rules. It should also publish more information about its security policies, including how it addresses security vulnerabilities and data breaches.

Telefónica, S.A. provides mobile, fixed-line broadband, and other services to more than 272 million mobile customers in Spain, Latin America, and internationally.[3]

Market cap: USD 44.0 billion[4]
BME: TEF
Domicile: Spain
Website: https://www.telefonica.com

Governance 94%

Telefónica significantly improved disclosure of its governance and oversight over human rights issues, earning the highest score in this category of any company in the 2019 RDR Index. It earned the highest score on all six indicators in the Governance category, and stood out for disclosing the clearest grievance and remedy mechanism of any company in the entire Index (G6). Notably, Telefónica was among the few companies evaluated to disclose that it assesses freedom of expression and privacy risks associated with enforcing its terms of service and its use of automated decision making technologies. However, it failed to disclose if it assesses risks associated with its targeted advertising practices and policies (G4).

Freedom of Expression 47%

Although Telefónica disclosed more about policies affecting freedom of expression than any other telecommunications company evaluated, it still fell short in key areas. The operating company Telefónica Spain's terms of service were somewhat difficult to find and understand (F1), and it was not clear whether users would be directly notified of changes (F2).[5] Telefónica improved its disclosure of how it responds to government requests, including those submitted by governments in foreign jurisdictions, but was less transparent about how it responds to requests it receives through private processes (F5). Telefónica provided some data about government requests it received and complied with (F6), but no data about requests received through private processes (F7).

Telefónica Spain was one of only two companies to commit to upholding net neutrality principles (F9). The company only partially disclosed the reasons why it may shut down or restrict access to its networks or certain protocols, though it was the only company to disclose both the number of requests it received and with which it complied (F10).

Privacy 49%

Telefónica made a number of improvements to its policies affecting privacy, but still lacked disclosure in a number of areas. Telefónica Spain revealed more than most of its peers about how it handles user information (P3-P8)—and made some key improvements—but could do more to clearly explain what user data it shares with third parties (P4), and options users have to control what data it collects and uses, including for purposes of targeted advertising (P7). It disclosed some information about its data retention policies, but did not disclose how long it retains personal data once users terminate their accounts (P6).

Telefónica was more transparent than most of its peers about how it handles government and private requests for user information (P10-P11). It clarified its process for responding to government requests for user data, including those submitted by foreign governments (P10), and provided some data on government requests for user information, though this data could be more comprehensive (P11). But like most companies in the Index, it lacked transparency about how it handles private requests for user information (P10, P11)—and did not disclose if it notifies users when government entities or other types of third parties request information (P12).

Telefónica Spain disclosed less than Deutsche Telekom, Vodafone UK, and AT&T about its security policies and practices (P13-P18). It disclosed that it has an internal security audit team, but failed to clearly disclose whether it limits or monitors employee access to user data (P13). It improved its disclosure of how it addresses security vulnerabilities by disclosing a program allowing researchers to report vulnerabilities (P14). However, the company lost points in this year's Index for disclosing less clear information about its policies for responding to data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Telefónica's performance in the 2018 Index, see: https://rankingdigitalrights.org/index2018/companies/telefonica

[3] "Telefónica in Numbers - FY2017" (Telefónica), Accessed January 15, 2019, https://www.telefonica.com/documents/153952/142035615/Telefonica-in-numbers-FY-2017.pdf/83eb9de4-42e5-a285-dfdb-581307080a4f

[4] Bloomberg Markets, Accessed April 18, 2019, https://www.bloomberg.com/quote/TEF:SM

[5] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Telefónica Spain.

Telecommunications company

Telenor ASA

Operating company evaluated:

- **Telenor Norway**

Services evaluated:

- **Telenor Norway (Prepaid mobile)**
- **Telenor Norway (Postpaid mobile)**
- **Telenor Norway (Fixed-line broadband)**

Rank

4

Score

45%

Rank among 12 telecommunications companies

Key findings

- Telenor disclosed strong corporate governance and oversight over human rights issues across its global operations, but still lacked transparency about its policies and practices affecting freedom of expression and privacy in key areas.
- Telenor lacked disclosure about how it handles government demands for user data or to block or filter content, although there are no legal barriers preventing it from being more transparent.
- The company did not reveal enough about what types of user data it collects and shares—or give clear enough options for users to control what is collected and shared about them.

Key recommendations

- **Be more transparent about government demands:** Telenor should disclose more detailed data about its compliance with government requests to restrict content or accounts, and to hand over user information.
- **Clarify handling of user data:** Telenor should clarify the types of data it collects, shares, and its policies for retaining user information. It should give users clear options to control what data the company collects and shares about them, including for the purposes of targeted advertising.
- **Improve remedy:** Telenor should be more accountable to users by strengthening its grievance and remedy mechanisms and ensuring that these procedures are accessible, predictable, and fully transparent.

Analysis

Telenor ranked fourth out of 12 telecommunications companies, scoring slightly higher than Deutsche Telekom, but lower than Telefónica, Vodafone, and AT&T.[1] The company—a newcomer to the RDR Index this year—is a member of the Global Network Initiative (GNI). However, while Telenor disclosed strong corporate governance and oversight over human rights issues and commitments across its global operations, it lacked sufficient transparency about its policies and practices affecting freedom of expression and privacy in key areas. Telenor was particularly opaque about how it handles government demands for user data, or to block content or deactivate accounts, despite there being no legal restrictions preventing the company from being more transparent in these areas.

Telenor ASA offers mobile and fixed-line broadband services in Scandinavia and Asia.

Market cap: USD 29.3 billion[2]
OSE: TEL
Domicile: Norway
Website: https://www.telenor.com

Governance 78%

Telenor received the fourth-highest score among telecommunications companies, after Telefónica, Orange, and Vodafone. It published a strong public commitment to respect freedom of expression and privacy as human rights (G1), and disclosed evidence of senior-level management over these issues within the company (G2). It disclosed that it conducts human rights impact assessments on existing products and services, but like most companies, failed to disclose whether it assesses risks associated with enforcing its terms of service, its use of automated decision-making technologies, or its targeted advertising policies and practices (G4). Telenor could also improve its grievance and remedy mechanisms: while it provided users with an option to submit complaints, including those related to freedom of expression and privacy, it offered no information about the number of complaints it received or any evidence that it provided users with a remedy (G6).

Freedom of Expression 34%

Telenor failed to disclose adequate information about policies and practices affecting users' freedom of expression, and was less transparent than Telefónica, Vodafone, and AT&T in a number of areas. While Telenor Norway was more clear than any other telecommunications operator in the Index about what types of content and activities are prohibited on its services (F3), it disclosed nothing about what actions it took to enforce these rules (F4).[3] Telenor also lacked sufficient transparency about how it handles third-party requests to block content or deactivate user accounts (F5-F7). Although telecommunications companies generally score poorly on these indicators, there is nothing preventing Telenor from being more transparent about how it handles these types of requests.

The company also disclosed very little about its network management policies, and failed to make a commitment to net neutrality principles (F9). But it disclosed more than most of its peers about its process for responding to government demands to shut down networks (F10).

Privacy 39%

Telenor disclosed less than most of its European peers about policies affecting users' privacy, and was particularly unclear about how it handles government demands for user data. It disclosed less than most of its European peers, except Orange, about its process for responding to government and private requests for user information (P10, P11)—and, like all telecommunications companies evaluated, it failed to disclose whether it would notify users of requests it receives for their information (P12).

Telenor Norway also fell short of clearly disclosing how it handles user information (P3-P8)—although it disclosed more than many of its peers, apart from Deutsche Telekom and Telefónica Spain. It did not fully disclose the types of data it collects (P3), or shares (P4), and disclosed almost nothing about its policies for retaining user information (P6). It also did not give users very clear options to control what data the company collects and shares about them, including for the purposes of targeted advertising (P7).

While Telenor Norway disclosed less about its security policies (P13-P18) than most of its European peers, it was one of the few telecommunications companies to provide some information about its process for responding to data breaches (P15). However, the company disclosed almost no information about how it addresses security vulnerabilities (P14).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/TEL:NO

[3] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Telenor Norway.

Internet and mobile ecosystem companies

Tencent Holdings Limited

Services evaluated:

- **QZone** [Social networking & blog]
- **QQ** [Messaging & VoIP]
- **WeChat** [Messaging & VoIP]
- **Tencent Cloud** [Cloud service]

Rank	Score	Difference
10	26%	^ 4.17

Rank among 12 internet and mobile ecosystem companies

Key findings

- Tencent revealed more information about its handling of user information than in the past, but still failed to publish sufficient information about policies affecting privacy.
- Tencent disclosed almost nothing—and less than all of its peers—about its governance processes to ensure respect for users' freedom of expression and privacy.
- Tencent disclosed nothing about how it responds to third-party requests to restrict user access to content and accounts, or to hand over user information.

Key recommendations

- **Improve disclosure of human rights due diligence:** Tencent should disclose more information about its human rights due diligence, including whether it conducts human rights risk assessments on new and existing services and when entering new markets.
- **Give users more control over their information:** Tencent should provide users with more options to access and control their own information.
- **Increase transparency about private requests:** Tencent should improve its disclosure of how it responds to private requests to restrict content or accounts and for user information.

Analysis

Tencent ranked tenth out of the 12 internet and mobile ecosystem companies evaluated in the 2019 Index, failing to disclose sufficient information about its policies and practices affecting users' freedom of expression and privacy.[1] Tencent did make key improvements to its privacy and security disclosures, particularly with regards to its disclosure of how it handles user information.[2] This progress could be attributed, in part, to new regulations requiring companies to be more transparent about their purposes for processing data.[3] However, it still failed to meet basic standards for respecting users' freedom of expression and privacy rights. While the Chinese internet environment is restrictive and the law forbids disclosures related to government demands, there are no legal barriers to prevent Tencent from improving its policies related to handling and securing user information.[4]

Tencent Holdings Limited provides a broad range of internet and mobile value-added services, online advertising services, and e-commerce transaction services to users in China and internationally. It is one of the world's largest internet companies.

Market cap: USD 474.4 billion[5]
SEHK: 700
Domicile: China
Website: https://www.tencent.com/

Governance 4%

Tencent disclosed almost nothing about its governance and oversight over its impact on users' human rights. While it committed to protect users' privacy, it fell short of committing to protect privacy as a human right (G1). Tencent disclosed no evidence of conducting human rights impact assessments, including if it assesses risks associated with its use of automated decision-making and targeted advertising (G4). It also failed to disclose if it engages with a range of stakeholders on these issues (G5), and did not appear to offer any grievance and remedy mechanisms allowing users to submit grievances if they feel the company has violated their freedom of expression or privacy (G6). While the legal and political environment in China is not conducive to companies making strong human rights commitments, Tencent can still improve its grievance and remedy mechanisms (G6), even if there are no regulatory improvements.

Freedom of Expression 14%

Tencent disclosed little about policies affecting freedom of expression, receiving the second-lowest score of all internet and mobile ecosystem companies in this category, after Baidu. The company's terms for its different services were not always easy to find or understand (F1), and did not indicate if and how it notifies users when it introduces changes to these terms (F2). Tencent disclosed limited information about its rules and how they are enforced (F3), and revealed nothing about actions it takes—such as removing content or deactivating accounts—to enforce its rules (F4). It also did not commit to notify affected users when the company restricts content or accounts (F8).

Tencent earned minimal points for disclosing limited information about how it responds to private requests to restrict access to content or accounts, but disclosed nothing about how it responds to such requests from governments (F5). It also did not publish any data about how many government or private requests for content or account restrictions it received or with which it complied (F6, F7).

Privacy 39%

Despite key improvements, Tencent still failed to publish sufficient information about policies affecting privacy. It disclosed a commitment to limit its collection of user information to what is directly relevant and necessary for QZone and QQ (P3) and that it will limit the use of user information to its original purpose, or otherwise obtain consent from users (P5). It improved its disclosure of options users have to control their own information by disclosing that QZone and QQ users can delete some types of user information (P7). However, the options users have to control and access their own information (P7, P8) remained insufficient. The company disclosed almost nothing about how long it retains user information, even though Chinese law does not prevent such disclosures (P6).

Tencent disclosed nothing about how it handles government and private requests for user information (P10-P12). While the Chinese legal and political environment makes it unrealistic to expect companies to disclose detailed information about government requests for user information, Tencent should be able to disclose if and when it shares user information via private requests and under what circumstances.

Tencent revealed less about its security policies than most other internet and mobile ecosystem companies. However, it improved its score by disclosing a policy of limiting employee access to user information (P13) for QZone and QQ, and a commitment to notify users in the event of a data breach (P15). While the company had one of the highest scores for disclosure on how it addresses security vulnerabilities (P14), it disclosed almost no information about encryption of user communications (P16), despite slightly improving its disclosure about the encryption of some user information on WeChat.

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Tencent's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/tencent

[3] "Personal Information Security Specification," December 2017, www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE

[4] "Freedom on the Net" (Freedom House, November 2018), freedomhouse.org/report/freedom-net/2018/china

[5] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/700:HK

Internet and mobile ecosystem companies

Twitter, Inc.

Services evaluated:

- **Twitter [Social networking & blog]**
- **Periscope [Video & photo sharing]**

Rank	Score	Difference
5	55%	^ 1.89

Rank among 12 internet and mobile ecosystem companies

Key findings

- Twitter was less transparent about policies and practices affecting freedom of expression and privacy than most of the U.S. internet and mobile ecosystem companies evaluated in the Index.
- It improved its disclosure of how it responds to government requests to restrict content or accounts by committing to carry out due diligence on such requests, but published limited data about the requests it received.
- Twitter failed to disclose sufficient information about its security policies, earning the second-lowest score on these indicators.

Key recommendations

- **Improve governance oversight:** Twitter should disclose if and how it conducts human rights impact assessments and offer clearer mechanisms to address users' privacy complaints.
- **Be more transparent about data retention policies:** Twitter should disclose more comprehensive information about what user data it retains and whether it deletes all user data when users terminate their accounts.
- **Clarify security policies:** Twitter should improve disclosure of its policies for responding to data breaches and encrypting user content and communication.

Analysis

Twitter ranked fifth out of 12 internet and mobile ecosystem companies, disclosing less about its processes to ensure respect for freedom of expression and privacy than most of its U.S. peers.[1] Twitter stood out for disclosing more than most of its peers regarding policies affecting users' freedom of expression, and it improved its disclosure slightly regarding its governance processes and options users have to obtain their user data, among other things.[2] However, despite these improvements, the company's performance continued to lag. It failed to disclose sufficient information about its policies to ensure the privacy and security of users' data, and of its governance processes in place to ensure respect for human rights compared to its U.S. peers. In addition, Twitter's disclosure declined in a few key areas, as the company revealed less comprehensive information about government requests it received to remove or restrict content or accounts and its data retention policies.

Twitter, Inc. operates a global social media platform with products and services that allow users to create, share, and find content on the Twitter social network, and livestream videos on Periscope. Twitter also provides advertising services and developer tools.

Market cap: USD 26.5 billion[3]
NYSE: TWTR
Domicile: USA
Website: https://twitter.com

Governance 50%

Despite some improvements, Twitter had weak disclosure of its governance and oversight over human rights issues, scoring lower than most U.S. internet and mobile ecosystem companies in this category. While it disclosed that it regularly engages with a range of stakeholders on freedom of expression and privacy issues (G5), Twitter is not a member of a multi-stakeholder initiative like the Global Network Initiative (GNI), which sets standards for how ICT companies should respect users' human rights. The company clarified that it educates employees about its privacy policies and disclosed a whistleblower policy to allow employees to submit privacy-related complaints, but not those related to freedom of expression (G3). Twitter disclosed some information about conducting human rights risk assessments when launching new products or entering into new markets, but did not disclose whether it conducts risk assessments related to its use of automated decision-making or targeted advertising (G4). Twitter's complaints mechanisms were stronger than Google's and Facebook's but it was less clear how users can submit grievances related to privacy (G6).

Freedom of Expression 60%

Although Twitter disclosed more than most of its peers about policies affecting users' freedom of expression—earning the second-best score in this category, behind Google—its overall score in this category declined slightly, and its disclosure fell short in a number of key areas.

Twitter earned the top score among its peers for clear disclosure of its rules and its processes for enforcing them (F3, F4, F8). It took a step forward by publishing a comprehensive Twitter Rules Enforcement report detailing what actions the company took to enforce its terms, but it was not clear if the company plans to publish this data on a regular basis, nor was the data available in a structured format (F4).[4] It also earned a score improvement by clarifying that when it restricts content or accounts for violating its rules, it will notify Twitter users attempting to access the restricted content of the reason for the restriction (F8).

Twitter also performed relatively well on its disclosure about how it handles government and private requests to restrict accounts, disclosing less than only Google and Verizon Media (F5-F7).[5] It clarified its process for responding to court orders and committed to carry out due diligence on government requests to remove or restrict content or accounts, including by pushing back against inappropriate or overbroad requests (F5). However, Twitter's data regarding content or account restriction requests no longer included as much information for Periscope (F6).

Privacy 55%

Twitter disclosed less about its privacy policies than most of its U.S. peers—including Microsoft, Apple, Google, and Verizon Media. It provided little information about its security policies, earning the second-lowest score on these indicators (P13-P18). Like most companies, it failed to disclose any information about how it responds to data breaches (P15). It lacked clear disclosure about its encryption practices (P16). It also disclosed less than all of its U.S. peers, aside from Facebook, about steps it takes to help users keep their accounts secure (P17).

Twitter disclosed less than most of its U.S. peers about how it handles government and private requests to hand over user data (P10-P12). It revealed some information about how it responds to government requests, but not private requests (P10). Twitter tied with Facebook and Apple for disclosing the most data on third-party requests for user information it received and complied with (P11). However, like other U.S. companies, it did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.[6]

On a positive note, Twitter earned the top score among internet and mobile ecosystem companies for disclosure of how it handles user information (P3-P9). It disclosed clear information about what types of user data it collects and how (P3). It clarified why it may track users across third party apps or websites (P9). It also disclosed an option for Periscope users to download some of their data (P8). Although it disclosed more than most companies about its data retention policies, Twitter was less transparent than in the previous year about if and when it deletes user information after users close their accounts (P6).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Twitter's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/twitter

[3] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/TWTR:US

[4] Twitter Rules Enforcement report, transparency.twitter.com/en/twitter-rules-enforcement.html

[5] Oath, which provides a range of communications services including Yahoo Mail and Tumblr, updated its name to Verizon Media on January 7, 2019. See: www.oath.com/2019/01/07/oath-is-now-verizon-media

[6] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Internet and mobile ecosystem companies

Verizon Media Inc.

Services evaluated:

- **Yahoo! Mail [Email]**
- **Tumblr [Social networking & blog]**

Rank	Score	Difference
2	61%	^ 3.23

Rank among 12 internet and mobile ecosystem companies

Key findings

- Verizon Media rose in the ranking to tie with Google for second place, and made a number of improvements to its disclosures.
- Verizon Media disclosed less data than all other U.S. internet and mobile ecosystem companies about the government and private requests it received for user information.
- Verizon Media was unclear about how it keeps user information secure, including how it handles data breaches.

Key recommendations

- **Be more transparent about policing of content:** Verizon Media should publish data on actions taken to restrict accounts and content that violate its rules.
- **Communicate more clearly about security:** Verizon Media should disclose how it responds to data breaches and be more forthcoming about how it keeps user information secure.
- **Clarify grievance and remedy mechanisms:** Verizon Media should clarify its grievance and remedy procedures for freedom of expression and privacy related concerns.

Analysis

Verizon Media rose in the ranking to tie with Google for second place among the 12 internet and mobile ecosystem companies evaluated,[1] falling slightly behind Microsoft.[2] As a member of the Global Network Initiative (GNI), Verizon Media was among the top performers in the Governance category, disclosing strong human rights commitments and providing evidence of implementing those commitments. The company's overall score increased by three percentage points, mainly due to improved disclosures about its freedom of expression and privacy policies.[3] Despite this progress, Verizon Media could still improve disclosure in key areas affecting users' human rights. It should be more transparent about how content is policed on its platforms and about its security practices. Verizon Media disclosed less data than all other U.S. internet and mobile ecosystem companies about government and private requests it received for user information.

Verizon Media Inc. (previously Oath, Inc.) is a subsidiary of Verizon Communications that provides a range of communications, sharing, and information and content services. Following the acquisition of Yahoo by Verizon Communications in June 2017, Verizon combined Yahoo and AOL branded services into a subsidiary called Oath. In January of 2019 Oath was renamed Verizon Media.

Market cap: USD 238.7 billion[4]
NasdaqGS: VZ
Domicile: USA
Website: https://www.verizonmedia.com

Governance 84%

Verizon Media received the second-highest governance score of all internet and mobile ecosystem companies, behind Microsoft. The company disclosed a clear commitment to respect freedom of expression and privacy in the context of international human rights frameworks (G1), evidence of senior leadership oversight of human rights issues (G2), and employee training and a whistleblower program addressing freedom of expression and privacy (G3). As a GNI member, it engages with stakeholders, including civil society, on freedom of expression and privacy issues (G5). It improved disclosure of its human rights impact assessments by clarifying that the board and senior executives oversee the results of such assessments (G4). However, like most companies, it failed to disclose whether it assesses risks to freedom of expression and privacy associated with the use of automated decision-making and targeted advertising.

Freedom of Expression 56%

Verizon Media disclosed more than Microsoft, Facebook, and Apple about its policies affecting users' freedom of expression, but still lacked transparency in key areas. It was less transparent about its process for enforcing its terms of service (F3) than all of its U.S. peers, other than Apple. Like most companies, it did not disclose any data about the volume or nature of actions it took to enforce its rules, such as removing content or restricting users' accounts (F4). Its policies regarding whether or not users are notified of account and content restrictions lacked clarity (F8). Verizon Media published terms of service that were easy to find and understand (F1). Its commitment to directly notify users of changes to the terms was clear for Tumblr but not for Yahoo! Mail (F2).

On a positive note, Verizon Media disclosed more than all of its peers about how it handles government and private requests to censor content or restrict accounts (F5-F7). While it provided less thorough disclosure of how it responds to requests filed through private processes than it did for government requests (F5), it provided more data about private requests (F7) than any other internet and mobile ecosystem company. It disclosed more data about government requests it received than any company aside from Google (F6).

Privacy 56%

Despite some improvements, Verizon Media did not disclose enough about its policies affecting users' privacy, disclosing less than Microsoft, Apple, and Google. It disclosed more about what user information it collects and shares (P3, P4), and for what purposes (P5) than it did about how long it retains user information (P6). Since the previous RDR Index, the company clarified its purposes for combining user information (P5) and provided Yahoo! Mail users with some options to control the collection of their data (P7). However, it provided less information than its U.S. peers about its tracking of users across the internet (P9), failing to disclose whether it respects user signals to opt out of tracking.

In contrast to improvements around how it handles user information, Verizon Media fell behind its U.S. peers for transparency around how it responds to third-party requests for user information (P10-P12). It clearly explained how it responds to government requests, (P10), but disclosed less data than its peers about the government and private requests it received for user information (P11).[5] Like other U.S. companies, Verizon Media did not divulge the exact number of requests received for user data under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), or the actions it took in response to these requests, since it is prohibited by law from doing so.

It was also less transparent than Apple, Microsoft, Kakao, Yandex, and Google about its security policies (P13-P18). While it disclosed that it has a security team that conducts audits, it provided no information about monitoring and limiting employee access to user information (P13). It was among seven internet and mobile ecosystem companies to disclose nothing about its policies for handling data breaches (P15).

Footnotes

[1] Verizon Media (formerly Oath) offers a range of services and media brands. RDR's Index evaluates two of these services: Yahoo! Mail and Tumblr. See: www.oath.com/2019/01/07/oath-is-now-verizon-media/

[2] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[3] For Yahoo's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/yahoo

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/VZ:US

[5] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), www.congress.gov/bill/114th-congress/house-bill/2048

Telecommunications company

Vodafone Group Plc

Operating company evaluated:

- **Vodafone UK**

Services evaluated:

- **Vodafone UK [Prepaid mobile]**
- **Vodafone UK [Postpaid mobile]**
- **Vodafone UK [Fixed-line broadband]**

Rank	Score	Difference
2	52%	^ 0.34

Rank among 12 telecommunications companies

Key findings

- Vodafone continued to be among the most transparent telecommunications companies in the RDR Index about its policies and practices that affect users' human rights.
- It was the only company to disclose comprehensive information about policies for handling data breaches.
- While it improved disclosure of what data it collects and for how long it is stored, Vodafone should be more transparent about how it handles and secures user information.

Key recommendations

- **Improve human rights due diligence:** Vodafone should demonstrate it carries out human rights risk assessments on existing products and services, as well as on its terms of service enforcement, its use of automated decision-making, and its targeted advertising policies and practices.
- **Clarify handling of user data:** Vodafone should be more transparent about its reasons for collecting and sharing user information, and clarify options users have to control what data is collected and shared about them.
- **Be transparent about third-party requests affecting freedom of expression:** Vodafone should better inform users about third-party requests (including from governments) to block content and to shut down networks, and disclose where laws may prevent it from being fully transparent about these types of requests.

Analysis

Vodafone's score in the 2019 RDR Index remained steady at 52%, but the company's ranking dropped to second place among telecommunications companies.[1] Despite improved privacy policy disclosure, it was outpaced in this area by some of its peers, including Telefónica—the only telecommunications company to outperform Vodafone in this year's RDR Index.[2] A member of the Global Network Initiative (GNI), Vodafone disclosed strong governance and oversight over human rights issues across its global operations, and excelled in key areas relative to its peers. It was the only company in the RDR Index to disclose comprehensive information about how it handles data breaches. It was one of only two telecommunications companies to commit to uphold net neutrality principles. The company made strides by spelling out the types of user information it collects and for how long it retains data on former users, but still did not disclose enough about how it handles user data. The company could also do more to explain how it handles and responds to government requests and other types of third party requests to block content and deactivate user accounts or to hand over user information.

Vodafone Group Plc provides telecommunications services in Europe, Asia, the Middle East, and Africa. The company serves 535.8 million mobile, 19.7 million fixed broadband, and 13.7 million TV customers.[3]

Market cap: USD 50.7 billion[4]
LSE: VOD
LSE: United Kingdom
LSE: https://www.vodafone.com

Governance 81%

Vodafone's strongest performance in this year's RDR Index was in the Governance category, where it received the third-best score among telecommunications companies. It disclosed a clear commitment to respect freedom of expression and privacy as human rights (G1) but fell behind many of its GNI peers for weak disclosure of human rights due diligence practices (G4). Vodafone disclosed that it conducts human rights impact assessments when entering new markets, but not whether it does so on existing products and services, the impacts of its terms of service enforcement, its use of automated decision making, or its targeted advertising policies or practices (G4). Vodafone earned the second highest score after Telefónica for disclosure of its grievance and remedy mechanisms (G6) although gaps remained. While Vodafone provided users with several options to submit complaints, including those related to freedom of expression and privacy, it offered no information about the number of complaints it received or any evidence that it provides users with remedy.

Freedom of Expression 45%

Vodafone received the second-highest score in the Freedom of Expression category among telecommunications companies, behind Telefónica—but its disclosure of policies affecting users' freedom of expression was inadequate in key areas. While Vodafone UK's terms of service for mobile and broadband were easy to understand (F1) it was not clear whether users are notified of changes (F2).[5] Vodafone disclosed less than AT&T and Telefónica about how it handles government and private requests to block content or restrict accounts, but it was one of the few telecommunications companies to disclose any information about its handling of these types of requests (F5-F7). While the company had strong disclosure of its process for handling government requests, it was less clear about how it handles similar private requests (F5). It also disclosed no data about the number of requests it received or with which it complied (F6, F7).

Vodafone UK tied with Telefónica Spain for the highest score on disclosure of network management policies, and disclosed a clear commitment to net neutrality (F9). It disclosed more than most of its peers, aside from Telefónica and Telenor, about its process for responding to network shutdown demands, although it did not disclose how many shutdown requests it received or with which it complied (F10).

Privacy 45%

Vodafone did not disclose enough about its policies affecting privacy—falling behind Deutsche Telekom, AT&T, and Telefónica—although it earned high marks on its security disclosures. Revisions to Vodafone UK's privacy policy to comply with the EU's General Data Protection Regulation (GDPR) did improve clarity about handling of user data (P3-P8) in a number of areas: it improved its disclosure of the types of information it collects (P3) and for how long it retains some user data after account termination (P6). But it still disclosed less overall than many of its peers—Deutsche Telekom, Telefónica Spain, Telenor Norway, and AT&T—about how it handles user information: it did not disclose whether users can control collection of their own information or whether users can delete some of this information (P7). While it explained how people can opt out of having their data used for advertising, it failed to disclose if targeted advertising is turned off by default (P7).

Vodafone disclosed less than AT&T and Telefónica about how it handles government and private demands for user information (P10, P11). It explained its process for responding to government requests for user data, but not how it responds to other types of third-party requests (P10). It failed to disclose if it notifies users when government entities or other third parties request their information (P12).

It disclosed more about its security policies (P13-P18) than any other telecommunications company aside from Deutsche Telekom—although it lost points in this year's RDR Index for being less transparent than previously about its internal policies for keeping user data secure (P13). Notably, it was the only company in the RDR Index to offer comprehensive information on its handling of data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] For Vodafone's performance in the 2018 Index, see: rankingdigitalrights.org/index2018/companies/vodafone

[3] 2018 Vodafone Group Plc Annual Report, www.vodafone.com/content/annualreport/annual_report18/downloads/Vodafone-full-annual-report-2018.pdf

[4] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/VOD:LN

[5] For most indicators in the Freedom of Expression and Privacy categories, RDR evaluates the operating company of the home market, in this case Vodafone UK.

Internet and mobile ecosystem companies

Yandex N. V.

Services evaluated:

- **Yandex Mail [Email]**
- **Yandex Search [Search engine]**
- **Yandex Disk [Cloud service]**

Rank	Score	Difference
8	32%	^ 5.67

Rank among 12 internet and mobile ecosystem companies

Key findings

- Despite key improvements, Yandex failed to disclose enough about policies affecting users' freedom of expression and privacy.
- It made notable strides by publishing a formal commitment to respect users' freedom of expression and privacy rights, but otherwise lacked evidence of strong governance and oversight over human rights commitments across the company's operations.
- Yandex disclosed almost nothing about how it handles government demands to restrict content or to hand over user data, although there are no legal barriers to disclosing at least some information about its processes for responding to these types of requests.

Key recommendations

- **Disclose more about government requests:** Yandex should disclose data about how it responds to government requests to remove content or deactivate accounts, and to hand over user data.
- **Improve governance oversight:** Yandex should put processes in place to strengthen institutional oversight over freedom of expression and privacy issues at the company.
- **Clarify handling of user information:** Yandex should disclose more about its handling of user information and its policies to keep user information secure.

Analysis

Yandex ranked eighth out of the 12 internet and mobile ecosystem companies evaluated, disclosing little about its policies and practices affecting freedom of expression and privacy.[1] The company made some substantive improvements, including by publishing a commitment to respect users' freedom of expression and privacy rights. It also improved its disclosure of policies affecting users' freedom of expression and privacy rights, but still lagged behind most other internet and mobile ecosystem companies evaluated. It disclosed almost nothing about government requests it receives for user information, and its disclosure of its freedom of expression policies lagged behind its Russian peer, Mail.Ru. While Yandex operates in an increasingly restrictive internet environment that discourages companies from publicly committing to protect human rights, the company could still be more transparent about key policies affecting users' freedom of expression and privacy.

Yandex N.V. provides a range of internet-based services in Russia and internationally, with products and services that include Yandex Search, the largest search engine in Russia, and email, cloud storage, and maps.

Market cap: USD 12.4 billion[2]
NasdaqGS: YNDX
Domicile: Russia
Website: https://www.yandex.com

Governance 29%

Yandex took a significant step forward by disclosing a commitment to respect users' freedom of expression and privacy rights in accordance with international human rights standards (G1), but otherwise had weak disclosure of its governance and oversight over human rights issues, scoring below most of the internet and mobile ecosystem companies evaluated.[3] It disclosed little about whether it carries out human rights due diligence—although it revealed that it considers how laws affect privacy in the jurisdictions where it operates (G4). Yandex disclosed that it provides a mechanism for users to submit freedom of expression and privacy related complaints, however, it failed to disclose its procedures for providing remedy (G6).

Freedom of Expression 22%

Yandex disclosed little about policies and practices impacting users' freedom of expression. The terms of service for Yandex Disk were easy to find, but not for Yandex Search, and its terms for Yandex Mail were more difficult to find than in the previous year (F1). These terms did not clarify if and how users would be notified of changes (F2). The company also lacked clear and comprehensive disclosure about the rules and how they are enforced, although it clarified that no government authorities or private entities receive priority consideration when flagging content to be restricted for violating the company's rules (F3). It also failed to disclose any data about actions it took to enforce its rules (F4).

Yandex disclosed some information about how it handles government and private requests to restrict content or accounts (F5-F7), although this disclosure was minimal. The company disclosed limited information about its process for responding to government and private requests for content and account restrictions (F5), and published no data on the number of government and private requests it receives or complies with (F6, F7). While Yandex had published some information about the content removed as a result of requests made under Russia's Right to Be Forgotten Law, it lost points since this information is now outdated (F7).

Privacy 38%

Despite some improvements, Yandex lacked transparency about policies affecting privacy in key areas. The company was especially opaque about how it handles user information. It revealed some information about what types of user data it collects (P3), shares (P4), and for what purpose (P5), but it revealed nothing about its data retention policies (P6), or if users can obtain a copy of the information the company holds about them (P8). It also failed to disclose whether and how it tracks users across the internet (P9). However, while Yandex lacked clarity about what options users have to control what data the company collects and shares about them, it was one of the few companies to disclose options users have to control how their data is used for targeted advertising (P7).

Yandex disclosed almost nothing about how it handles third-party requests for user information (P10-P12). The company earned some credit for improving its disclosure of how it responds to government requests for user data, but its disclosure about private requests was less clear (P10). It provided no data about these types of requests that it received and with which it complied (P11). Since Russian authorities may have direct access to communications data, companies may not be aware of the frequency or scope of user information accessed by authorities.[4] Still, it could disclose its processes for dealing with government requests in the cases they occur.

On a positive note, Yandex had stronger disclosure of its security policies than most internet and mobile ecosystem companies (P13-P18). It received the second-highest score after Apple for its disclosure of its encryption policies (P16), and provided relatively strong disclosure about its bug bounty program for addressing security vulnerabilities (P14). Like most of its peers, Yandex provided no information about how it responds to data breaches (P15).

Footnotes

[1] The research period for the 2019 Index ran from January 13, 2018 to February 8, 2019. Policies that came into effect after February 8, 2019 were not evaluated in this Index.

[2] Bloomberg Markets, Accessed April 18, 2019, www.bloomberg.com/quote/YNDX:US

[3] "About Yandex," yandex.com/company/general_info/yandex_today

[4] Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," The Guardian, September 8, 2015, www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet