RANKING DIGITAL RIGHTS

2017 CORPORATE ACCOUNTABILITY INDEX

The Ranking Digital Rights 2017 Corporate Accountability Index ranks 22 of the world's most powerful telecommunications, internet, and mobile companies on their disclosed commitments, policies, and practices that affect users' freedom of expression and privacy.

rankingdigitalrights.org/index2017

MARCH 2017

Acknowledgments

Ranking Digital Rights Staff:

- Rebecca MacKinnon, Project Director
- Amy Brouillette, Research and Editorial Manager
- Lisa Gutermuth, Program Manager
- Laura Reed, Senior Research Analyst
- Ilana Ullman, Policy and Communications Analyst
- Nathalie Maréchal, Senior Fellow
- Andrea Hackl, Senior Fellow

We also wish to acknowledge former team members for their work in researching and implementing revisions to the 2017 Index methodology: Priya Kumar, Research Analyst; Allon Bar, Policy and Engagement Manager; Revati Prasad, PhD student Annenberg School for Communication, University of Pennsylvania. Special thanks to Chris Ritzo, Senior Technologist at Open Technology Institute.

Contributing researchers: Afef Abrougui, Shazeda Ahmed, Félix Blanc, David Bravo, Alex Comninos, Matt J. Duffy, Luis Fernando García, Kwangjun Heo, Elonnai Hickok, Sergei Hovyadinov, Danielle Kehl, Shabina S. Khatri, Kelly Kim, Priya Kumar, Tetyana Lokot, Laura A. Mora Ardila, Mohamad Najem, Carly Nyst, Julie Owono, Gisela Pérez de Acha, Revati Prasad, Mingli Shi, Jiwon Sohn, Seamus Tuohy, Hu Yong, Benjamin Zhou.

Design and layout: Alison Yost, Senior Communications Manager, New America's Open Technology Institute; Joanne Zalatoris, Communications Assistant, New America.

Cover design and graphics concept: Olivia Solis, SHARE Foundation.

Advisory council: We are also grateful for the support and advice of our advisory council members: **https://rankingdigitalrights.org/who/advisory-council/**.

Special thanks: Matthew Barg, Research Products, Sustainalytics.

Funders: The 2017 Corporate Accountability Index was supported by: John D. and Catherine T. MacArthur Foundation, Ford Foundation, Open Society Foundations, U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, Open Technology Fund (Information Controls Fellow), and the Mozilla Foundation (Open Web Fellowship). For a full list of current and former project funders and partners, see: **https://rankingdigitalrights.org/who/partners/**.

About Ranking Digital Rights

Ranking Digital Rights is a non-profit research initiative housed at New America's Open Technology Institute. We work with an international network of partners to set global standards for how companies in the information and communications technology (ICT) sector should respect freedom of expression and privacy.

For more about Ranking Digital Rights and the Corporate Accountability Index, please visit **https://rankingdigitalrights.org**.

For more about New America, please visit **https://www.newamerica.org/**.

For more about the Open Technology Institute, please visit **https://www.newamerica.org/oti/**.

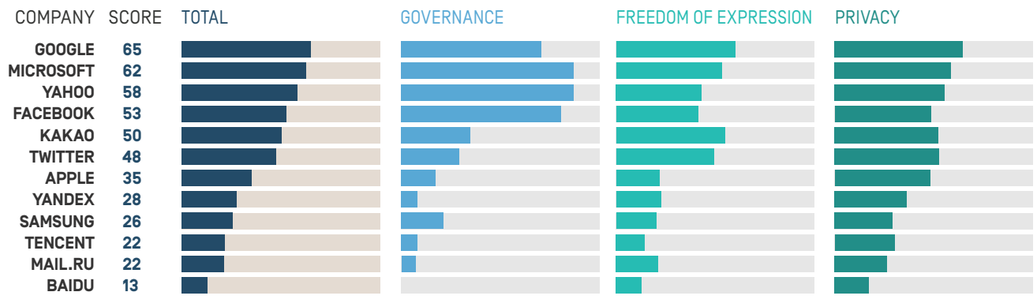
Contents

Contents, cont.

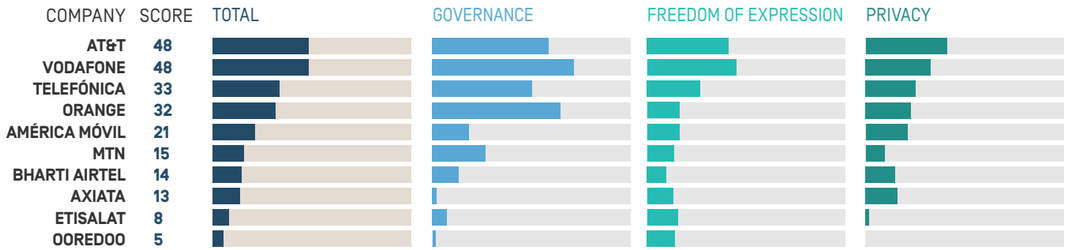
Contents, cont.

2017 CORPORATE ACCOUNTABILITY INDEX

● INTERNET AND MOBILE



● TELECOMMUNICATIONS



EXECUTIVE SUMMARY

The Ranking Digital Rights 2017 Corporate Accountability Index evaluates 22 of the world's most powerful internet, mobile, and telecommunications companies on disclosed commitments and policies affecting freedom of expression and privacy.

Together, the companies evaluated in the Index offer products and services that are used by at least half of the world's 3.7 billion internet users. **We regret to report that companies do not disclose enough information to their users about policies and practices affecting freedom of expression and privacy.** As a result, most of the world's internet users lack the information they need to make informed choices. We are also pleased to report, however, that many companies have made meaningful improvements since our inaugural Index was launched in late 2015.

This Index builds on the 2015 Index, adding six new companies and expanding the methodology to include what we call "mobile ecosystems." Companies were evaluated on 35 indicators examining disclosed commitments and policies affecting freedom of expression and privacy, including corporate governance and accountability mechanisms. To view in-depth results and data visualizations, download full datasets, and access related resources, news, and updates, please visit: rankingdigitalrights.org.

Key Findings

Company disclosure was inadequate across the board. Similar to the 2015 results, the average score for all companies evaluated was just 33 percent. The highest overall score in the 2017 Index was 65 percent. While examples of good practice could be found across the Index, all companies failed to sufficiently disclose policies affecting users' freedom of expression and privacy. Even the better performing companies had significant gaps in disclosure on key issues that affect what a user can and cannot say or do, as well as who knows what about their activities. Some highlights:

- **Google** and **Microsoft** were the only companies in the entire Index to score more than 60 percent overall. However, Google's lead over the other companies ranked near the top of the Index narrowed since 2015, while Microsoft moved from third to second place, primarily due to improved disclosures about policies affecting freedom of expression.

- **AT&T** and **Vodafone** tied for the highest score among the 10 telecommunications companies evaluated. Vodafone scored better on disclosures related to its governance mechanisms as well as policies affecting freedom of expression. AT&T offered more detailed disclosure on policies and practices affecting users' privacy.

- **Apple** ranked seventh among the 12 internet and mobile ecosystem companies evaluated. A major reason for this relatively low score was poor disclosure about the company's commitments and policies affecting users' freedom of expression. Next to its peers, Apple also offered little disclosure about how it has institutionalized commitments to users' rights through corporate governance, oversight, and accountability mechanisms.

- **Kakao**, a South Korean company that offers internet search, email, and mobile chat services, earned high scores on 10 of the 35 indicators across the Index.

The Index offers a roadmap for companies to demonstrate greater respect for their users' rights around the globe. After analyzing this year's data we have identified a number of specific concerns:

- **Mobile ecosystems: We don't know enough about the impact of smartphones on our digital rights.** We evaluated three mobile ecosystems: Apple's iOS ecosystem, the Google Android mobile ecosystem, and Samsung's implementation of Android. All three offered poor disclosure about policies affecting freedom of expression and privacy. Google disclosed the most information across the board about policies and practices affecting Android smartphone users' freedom of expression and privacy. Apple's iOS mobile ecosystem was more competitive than Samsung on privacy-related disclosures and generally offered better disclosure than Samsung across the board.

- **Freedom of expression is getting short-changed.** How do company actions affect our ability to publish, transmit, or access content? With a couple of notable exceptions, most companies disclosed less about policies that affect users' freedom of expression than about policies affecting privacy. This includes information about users' ability to publish, transmit, or access content that may be constrained or blocked—and under whose authority and for what reasons.

- **Handling of user information is opaque.** How and for what purpose is our information collected, shared, retained, and used? If somebody were to build a profile on you using this information, what would it look like? Companies don't disclose enough for users to understand risks and make informed choices.

- **Security commitments lack sufficient evidence.** In order to trust a service, we need to know that credible efforts are being made to secure our information. Most companies communicate less about what they are doing to protect users' security than about what users should do to protect themselves. Disclosure about company policies for informing affected parties about data breaches was especially poor.

Recommendations for Companies:

Companies seeking to improve trust and credibility can take a number of practical and immediate steps to improve disclosures that demonstrate respect for users' freedom of expression and privacy. These steps include:

- **Provide concrete evidence that the company has institutionalized its commitments.** While it is important for company leaders to demonstrate strong personal commitments to users' rights, it is even more important that such commitments be clearly institutionalized. Otherwise, how do users know whether policies and practices will change or stay the same after key individuals leave the company?

- **Undertake due diligence.** Does the company have a systematic way to understand and address the impact of products, services, and business operations on users' rights? Responsible companies disclose that they conduct human rights impact assessments (HRIAs) that cover freedom of expression and privacy. In order to be credible, the quality and scope of these assessments should be verified by an independent multi-stakeholder organization committed to human rights principles.

- **Explain to users why speech, access to information, or access to service may be blocked or constrained.** Who has the ability to ask the company to remove or block content or otherwise restrict speech? How does the company handle these requests? Are there effective grievance and remedy mechanisms? Companies must be transparent and accountable about the circumstances under which access to a service may be denied, or content is restricted or blocked.

- **Inform users about what happens to their information.** If somebody were to create a profile based on the information a company holds about a person, what would it look like? What organizations, governments, or other entities have access to users' information, under what circumstances? Companies must disclose enough details to answer these questions so that users can make informed decisions about what services to use.

- **Demonstrate a credible commitment to security.** Does the company maintain industry standards of encryption and security, conduct security audits, monitor employee access to information, and educate users about threats?

- **Develop effective grievance and remedy mechanisms.** Companies should have channels for users and other affected parties to file grievances if they feel that their rights to freedom of expression or privacy have been violated as a result of company actions. Companies should also have clearly disclosed processes for responding to complaints and providing appropriate redress.

It is important to remember that full corporate accountability will only be achieved when governments are also held accountable. (For our recommendations for governments, see Chapter 8).

Everyone—companies, civil society activists, citizens, responsible investors, and policy-makers—must all work together to build legal, regulatory, and corporate standards that make it possible to protect and respect human rights.

> **The Index offers a roadmap for companies to demonstrate greater respect for their users' rights around the globe.**

ABOUT THE RANKING DIGITAL RIGHTS CORPORATE ACCOUNTABILITY INDEX

Ranking Digital Rights (RDR) produces a Corporate Accountability Index that ranks the world's most powerful internet, mobile, and telecommunications companies' disclosed commitments and policies affecting users' freedom of expression and privacy. The Index is a standard-setting tool aimed at encouraging companies to abide by international human rights principles and standards for safeguarding freedom of expression and privacy.

The standards the Index uses to evaluate companies build on more than a decade of work by the human rights, privacy, and security communities. These standards include the U.N. Guiding Principles on Business and Human Rights,[1] which affirm that while governments have a duty to protect human rights, companies have a responsibility to respect human rights. The Index also builds on the Global Network Initiative principles[2] and implementation guidelines,[3] which address ICT companies' specific responsibilities towards freedom of expression and privacy in the face of government demands to restrict content or hand over user information. The Index further draws on a body of emerging global standards and norms around data protection, security, and access to information. The Index data and analysis inform the work of human rights advocates, policymakers, and responsible investors, and are used by companies to improve their own policies and practices.

In 2015, RDR launched its inaugural Corporate Accountability Index, which ranked 16 internet and telecommunications companies.[4] For the 2017 Index, RDR expanded the ranking to cover additional types of companies and services, including those that produce software and devices that create what we call "mobile ecosystems."[5] As a result, we expanded the methodology, adding new indicators and elements to account for the potential threats to users' freedom of expression and privacy that can arise from the use of networked devices and software.[6]

The RDR team also further refined the methodology based on a detailed review of the raw data from the 2015 Index, as well as in consultation with stakeholders from civil society, academia, the investor community, and the companies themselves. Due to these revisions, we are not able to produce direct year-on-year assessments of company performance between the 2015 and 2017 Index. We can and do, however, note cases in which a company's commitments and disclosures have improved.[7]

1. INDEX METHODOLOGY

The 2017 Index measures if and how companies disclose their commitments, policies, and practices that affect users' freedom of expression and privacy across 35 indicators in three main categories: **Governance**, **Freedom of Expression**, and **Privacy**. Each category contains **indicators** measuring company disclosure for that category; each indicator is comprised of a series of **elements** that measure company disclosure for that indicator.[8]

1.1 Index Categories

- **Governance (G):** This category contains six indicators measuring company disclosure of commitments to freedom of expression and privacy principles along with measures taken to implement those commitments across the company's global operations.[9]

- **Freedom of Expression (F):** This category contains 11 indicators measuring company disclosure of policies that affect users' freedom of expression.[10]

- **Privacy (P):** This category contains 18 indicators measuring company disclosure of policies and practices that affect users' privacy rights.[11]

1.2 Company Types

While every company we examined has attributes that make it unique, for the purpose of research and scoring, we divided the 22 companies into two groups.

Internet and mobile ecosystems: These company types were evaluated together because Google is both an internet company and a mobile ecosystem company, and Apple also offers services such as iMessage and iCloud. We did not evaluate hardware attributes of devices, focusing our assessment on disclosures pertaining to the newest devices offered by those companies and their operating systems. The freedom of expression and privacy issues faced by mobile cloud data and operating systems overlap with the issues faced by traditional internet services. Additional elements relevant only to mobile ecosystems were added to some indicators. For each company we examined up to four services, as follows:

- **Apple (U.S.)** — iOS mobile ecosystem, iMessage, iCloud

- **Baidu (China)** — Baidu Search, Baidu Cloud, Baidu PostBar

- **Facebook (U.S.)** — Facebook, Instagram, WhatsApp, Messenger
- **Mail.Ru (Russia)** — VKontakte, Mail.Ru email, Mail.Ru Agent
- **Microsoft (U.S.)** — Bing, Outlook.com, Skype
- **Kakao (South Korea)** — Daum Search, Daum Mail, KakaoTalk
- **Google (U.S.)** — Search, Gmail, YouTube, Android mobile ecosystem
- **Samsung (South Korea)** — Samsung implementation of Android
- **Tencent (China)** — QZone, QQ, WeChat
- **Twitter (U.S.)** — Twitter, Vine, Periscope
- **Yahoo (U.S.)** — Yahoo Mail, Flickr, Tumblr
- **Yandex (Russia)** — Yandex Mail, Yandex Search, Yandex Disk

Telecommunications companies: For these companies, we evaluated global group-level policies for relevant indicators, plus the home-country operating subsidiary's pre-paid and post-paid mobile service, and fixed-line broadband service where offered, as follows:

- **América Móvil (Mexico)** — Telcel
- **AT&T (U.S.)** — AT&T Mobile, AT&T Broadband
- **Axiata (Malaysia)** — Celcom
- **Bharti Airtel (India)** — India Airtel Mobile, India Airtel Broadband
- **Etisalat (UAE)** — Etisalat UAE Mobile, Etisalat UAE Broadband
- **MTN (South Africa)** — MTN South Africa Mobile
- **Ooredoo (Qatar)** — Ooredoo Qatar Mobile, Ooredoo Qatar Broadband
- **Orange (France)** — Orange France Mobile, Orange France Broadband
- **Telefónica (Spain)** — Movistar Mobile, Movistar Broadband
- **Vodafone (UK)** — Vodafone UK Mobile, Vodafone UK Broadband

1.3 What the Index Measures

Corporate-level commitment to freedom of expression and privacy: We expect companies to make an explicit statement affirming their commitment to freedom of expression and privacy as human rights, and to demonstrate how these commitments are institutionalized within the company. Companies should disclose clear evidence of: senior-level oversight over freedom of expression and privacy, and employee training and whistleblower programs addressing these issues; human rights due diligence and impact assessments to identify the impacts of the company's products, services and business operations on freedom of expression and privacy; systematic and credible stakeholder engagement, ideally involving membership in a multi-stakeholder organization committed to human rights principles including freedom of expression and privacy; a grievance and remedy mechanism enabling users to notify the company when their freedom of expression and privacy rights have been affected or violated in connection with the company's business, plus evidence that the company provides appropriate responses or remedies.

Terms of service and privacy policies: We expect companies to provide terms of service agreements and privacy policies that are easy to find, understand, and available in the primary languages of the company's home market, and accessible to people who are not account holders or subscribers. We also expect companies to clearly disclose whether and how they directly notify users of changes to these policies.

Terms of service enforcement: We expect companies to clearly disclose what types of content and activities are prohibited and their processes for enforcing these rules. We also expect companies to publish data about the volume and nature of content and accounts they have removed or restricted for violations to their terms, and to disclose if they notify users when they have removed content, restricted a user's account, or otherwise restricted access to content or a service.

Handling user information: We expect companies to clearly disclose each type of user information they collect, share, for what purposes they collect and share it, how they collect this information, and for how long they retain it. Indicators also look for companies to offer users options to control what is collected and to obtain all of the information a company holds on them.

Handling of government and private requests: We expect companies to clearly disclose how they respond to requests by governments and private entities to restrict content and user accounts and to hand over user information. We also expect companies to produce data about the types of requests they receive and the number of these requests with which they comply. Companies should notify users when their information has been requested.

Identity policies: We expect companies to disclose whether they ask users to verify their identities using a government-issued ID or other information tied to their offline identities. The ability to communicate anonymously is important for the exercise and defense of human rights around the world. Requiring users to provide a company with identifying information presents human rights risks to those who, for example, voice opinions that do not align with a government's views or who engage in activism that a government does not permit.

Network management and shutdowns: Telecommunications companies can shut down a network, or block or slow down access to specific services on it. We expect companies to clearly disclose if they engage in practices that affect the flow of content through their networks, such as throttling or traffic shaping. We expect companies to clearly disclose their policies and practices regarding network shutdowns. We also expect companies to explain the circumstances under which they might take such action and to report on the requests they receive to take such actions.

1.4 Evaluation

The Index evaluates company disclosure of the overarching "parent," or "group," level as well as well as those of selected services and/or local operating companies (depending on company structure). The evaluation includes an assessment of disclosure for every element of each indicator, based on one of the following possible answers: "full disclosure," "partial," "no disclosure found," "no," or "N/A."

Scoring: Companies receive a cumulative score of their performance across all Index categories, and results show how companies performed by each category and indicator. Scores for the Freedom of Expression and Privacy categories are calculated by averaging scores for each service. Scores for the Governance category indicators include parent- and operating-level performance (depending on company type).

Points:

- Full disclosure = 100
- Partial = 50
- No disclosure found = 0
- No = 0
- N/A excluded from the score and averages

Research for the 2017 Index was conducted from September 1, 2016 through January 13, 2017. New information published by companies after that date was not evaluated. (For more information on the Index methodology, company selection, and evaluation and scoring, see the Appendix, page 90).

2. INTRODUCTION

The 22 companies ranked in this Index collectively affect the lives of billions of people who use the internet across the world. The products and services they offer connect and empower people in unprecedented ways, but they can also be misused to undermine freedom of expression and privacy.

Recent research points to an erosion of trust. The Internet Society warns that the continued rise in data breaches will not only harm individuals and damage public trust, but also could result in "lower and more selective use of the internet."[12] Roughly half of Americans surveyed in 2016 by the Pew Research Center said they did not trust either the government or social media services to protect their data.[13] In a recent World Economic Forum survey of internet users in Brazil, China, Egypt, Germany, South Africa, and the United States, over half of global respondents agreed that user controls over the sharing of their personal information are inadequate. Less than half agreed that service providers valued users' privacy, or were reasonable in the use of their personal data. Greater transparency was rated highly as one of the key ways that companies can win users' trust.[14]

A 2016 report by the Global Commission on Internet Governance further warns that an internet that fulfills its economic and social potential, and on which fundamental human rights such as privacy and freedom of expression are protected, will be elusive unless all actors that shape the internet take responsibility for achieving that vision and are held accountable to it.[15] While many research organizations (Freedom House, the World Wide Web Foundation, Article 19, the Association for Progressive Communications, and others) collect and analyze comparative data that can be used to hold governments accountable for whether they are protecting or violating digital rights, the Ranking Digital Rights Corporate Accountability Index is the only global benchmark of ICT sector companies' commitments and policies affecting freedom of expression and privacy.[16]

Both rights are part of the Universal Declaration of Human Rights[17] and are enshrined in the International Covenant on Civil and Political Rights.[18] They apply online as well as offline. According to the U.N. Guiding Principles on Business and Human Rights, governments have the primary duty to protect human rights, but companies also have a responsibility to respect human rights. To put it concretely:

"Business enterprises need to know and show that they respect human rights. They cannot do so unless they have certain policies and processes in place."[19]

Ranking Digital Rights (RDR) does not have the capacity to carry out technical testing and field research to document the real-life impacts that the world's most powerful internet, mobile, and telecommunications companies have on people all over the world. We are, however, able to carry out a comparative evaluation of companies' commitments, policies, and disclosed processes affecting users' freedom of expression and privacy. We believe that public commitment and disclosure of basic policies is an essential baseline from which to evaluate companies' respect for human rights.

While companies that provide thorough disclosure of good policies and processes are not immune to problems by any means, their disclosures provide evidence to users and other stakeholders that the company has not only made commitments, but has also made systematic efforts to implement them. Such efforts should include due diligence to identify and anticipate problems and oversight mechanisms to ensure that executives, managers, and employees are held appropriately accountable. Having clearly disclosed policies in place not only enables companies to better manage risks and prevent harms, it also enables users to make informed choices about what services to use in order to manage their own risks and needs related to their personal exercise of freedom of expression and privacy rights.

There is much remedial work to be done. Yet if one looks more closely at the Index data, at particular clusters of indicators and companies, and even within specific indicators, one can find examples of many praiseworthy efforts and even some model practices. Even the lowest-scoring companies are disclosing at least something that is good and worth emulation by their peers.

A particular bright spot since the first Index was published in 2015 is an improvement in the quality and scope of "transparency reporting," as the practice has come to be called across much of the industry.[20] Since Google published its first report in 2010, transparency reporting has become the standard vehicle through which companies can "showcase their values and commitments to protecting user rights."[21]

Several of the indicators in both the Freedom of Expression and Privacy categories of the Index examine different facets of transparency reporting, both as the practice affects users' ability to access and share content (freedom of expression) and as it affects the extent to which governments and other third parties are able to request and obtain access to user information and communications (privacy). We have found that companies are gradually improving the quality and scope of disclosure about how they handle government and other third-party requests for user information, or to block, remove, or otherwise restrict content or user accounts. The higher-scoring companies in the Index are among the world's industry leaders in transparency reporting. Some have lobbied governments for the right to publish even more information about the requests they receive.

Taken as a whole, the Ranking Digital Rights Corporate Accountability Index measures the minimum standards companies should meet in order to fulfill their commitments to respect freedom of expression and privacy rights. Company "report cards" provide a snapshot of each company's performance and recommendations for improvement (see page 48). Our key findings section serves as a broader guide to what some companies are doing relatively well and where the most remedial effort is needed. This report and the data freely available on the website are meant to be used not only by companies themselves but also by investors, policymakers, civil society advocates, researchers, journalists, and any technology user who wants to make informed choices.

3. COMPANY DISCLOSURE IS INADEQUATE ACROSS THE BOARD

While examples of good practice could be found across the Index, all companies evaluated failed to disclose enough information to their users about policies and practices affecting freedom of expression and privacy.

The Ranking Digital Rights Corporate Accountability Index measures the minimum standards companies should meet in order to fulfill their commitments to respect freedom of expression and privacy rights.

> **Most of the world's internet users lack the information they need to make informed choices.**

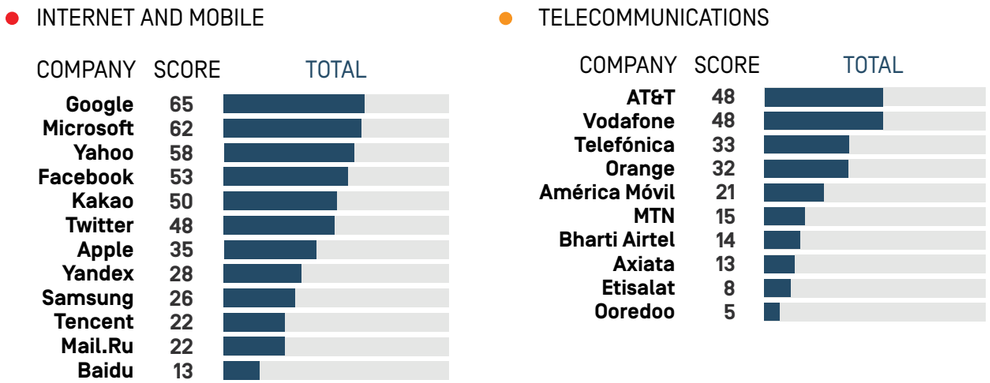
Similar to the 2015 Index results, the average score for all 22 companies evaluated was just 33 percent—and no company in the 2017 Index scored more than 65 percent overall.[22] Even the best performing companies had significant gaps in their disclosure. Despite some improvements, collectively these companies failed to meet the benchmarks of transparency. As a result, most of the world's internet users lack the information they need to make informed choices.

3.1 The Ranking

Google ranked first again, but Microsoft is closing in. Google continued to lead the Index—although there is much room for improvement. Microsoft, which placed third in 2015, ranked second this year, just three percentage points behind Google.[23] This shift was due in part to Microsoft's improved disclosure since the 2015 Index of policies affecting freedom of expression in particular and other human rights concerns in general. Meanwhile, Google's lead in the Index narrowed in 2017 due to the addition of Google's Android mobile operating ecosystem, for which the company disclosed information less than it did for the other Google services evaluated. Google also suffered from a decline in clarity about its commitments and their implementation at the corporate level.

AT&T and Vodafone tied for first place among telecommunications companies. AT&T and Vodafone earned the top scores among telecommunications companies to tie for the number one ranking in the 2017 Index. Vodafone outscored AT&T on implementation of its commitments at the corporate governance level and its disclosure of specific freedom of expression-related policies. But AT&T surpassed Vodafone in the Privacy category, with better disclosure of

Figure 1 | 2017 Index Ranking



its security practices, as well as more detailed transparency reporting about government requests for user information. Laws in some of Vodafone's operating markets prevent it from reporting the same amount of detail.

3.2 New Companies, New Insights

The addition of six new companies to the Index—Apple, Baidu, Ooredoo, Telefónica, Samsung, and Yandex—allowed for new points of analysis.

Including Apple and Samsung alongside Google rounded out the new mobile ecosystem service category. The three mobile ecosystems evaluated were Google Android, Apple iOS, and Samsung's implementation of Android. Findings showed that all three mobile ecosystems failed to sufficiently disclose policies affecting users' freedom of expression and privacy, though overall Google had stronger disclosure than the other two mobile ecosystems (see page 23).

Telefónica, which outranked Orange but came in behind Vodafone and AT&T, provided additional information about industry practices in the telecommunications field, and led the industry on several indicators. Telefónica led all 22 companies for its disclosure on responding to data breaches (see page 40). Its disclosure of policies related to network shutdowns was also among the more comprehensive of all telecommunications companies evaluated (see page 32).

To read the analysis of each company's individual performance, see "Company Report Cards," starting on **page 46**.

The addition of Yandex and Baidu revealed that even in restrictive legal and political environments like Russia and China, companies have room to make policy choices. In the Chinese context, Tencent outperformed Baidu, particularly in the Privacy category. While state secrets laws make it unrealistic to expect Chinese companies to reveal information on government requests to delete content or accounts or hand over user information, there is no legal obstacle to disclosing a range of information about how the company handles user information in the commercial context, as well

To read more about our evaluation of mobile ecosystems, and comparisons of Russian and Chinese internet companies, go to the 2017 Index website at: rankingdigitalrights.org/index2017.

as the security measures it takes to protect user information.

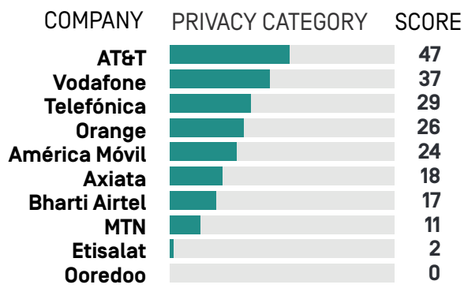
Similarly, the greatest differences between the Russian companies were found in the Privacy category, where Yandex significantly outpaces Mail.Ru. Yandex was one of the top-performing companies for its disclosure of its security policies, but could significantly improve its disclosure of how it handles user information. But Mail.Ru shared more information about its purpose for collecting and sharing information, and its data retention practices.

3.3 EU and Privacy

Despite the European Union's strong data protection laws, European telecommunications companies had inconsistent disclosure on policies affecting users' right to privacy.

While Vodafone (UK), Telefónica (Spain), and Orange (France) are subject to the same EU data protection requirements, there were notable differences in how and to what extent these companies publicly disclosed policies and practices affecting user privacy. Different countries' national security laws inhibit transparency about government requests for user information to varying extents and contribute to some of the differences. Other differences are entirely within the companies' own control.

Figure 2 | Telecommunications Companies



- **Transparency reporting about government requests:** Although AT&T and Vodafone tied for the top-ranked spot among telecommunications companies, AT&T led all other telecommunications companies in the Privacy category largely because of its comparatively high levels of disclosure about how it handles government requests for user information. Its transparency reports provided much more detail on the volume and nature of government requests for user information. While Vodafone and Orange disclosed that laws in some of their operating markets prevent them from reporting as many details about government requests, our analysis found that all three EU-based companies still have much room to improve their disclosure of policies for responding to government and private requests for user information.

- **Handling of user information:** All companies, and especially telecommunications companies, lacked clear disclosure of how they handle user information (see page 34). However, the EU-based telecommunications companies had insufficient and inconsistent disclosure of how they collect, share, retain, and otherwise handle user information. While they may be communicating with regulators about data collection, handling, and sharing to ensure compliance with the law, they do not communicate clearly with their own users, if one is to assume that most users are not fluent in European telecommunications and privacy law. From a human rights perspective it is insufficient for a company to communicate with regulators but not to communicate clearly with users about what happens to information that could be used to profile and track their attributes and activities.

3.4 Governance

When companies work together and with stakeholders to implement human rights commitments, they make a measurable difference.

While even the highest scores in the Index showed major room for improvement, some of the top-scoring companies shared one commonality: all are members of either the Global Network Initiative (GNI) or the Telecommunications Industry Dialogue (TID), organizations whose company members commit to uphold principles of freedom of expression and privacy.[24] Additionally, GNI conducts an assessment of whether members have implemented the principles satisfactorily. It has multi-stakeholder membership and is governed by a multi-stakeholder board.

The 2017 Index data showed that GNI and TID member companies performed better on indicators in the Governance category—measuring the institutionalization of corporate-level commitments to freedom of expression and privacy than all other companies (see Figure 3).[25] However, in other areas of the Index, GNI or TID membership was not necessarily a predictor of strong performance. For example, the South Korean company, Kakao, earned high scores on 10 of the 35 indicators across the Index.

Among internet and mobile companies, Microsoft, Yahoo, Facebook, and Google—all GNI members—had the highest scores in the Governance category, leading the rest of the companies by a significant gap. Facebook, which underwent its first full GNI assessment in 2016, saw a substantial improvement in its Governance scores since it was evaluated in the 2015 Index.[26]

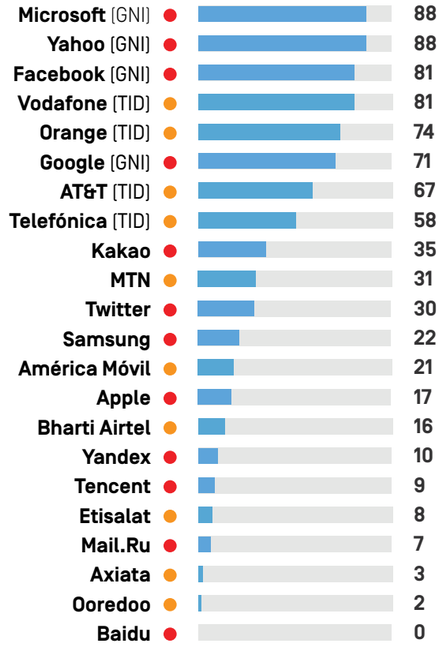
What Do Governance Indicators Measure?

The Governance category of the Index evaluates whether companies demonstrate that they have oversight, due diligence, and accountability processes in place to ensure that freedom of expression and privacy are respected throughout the company's operations. For a company to perform well on this category, its disclosure should at least follow, and ideally surpass, the U.N. Guiding Principles on Business and Human Rights and other industry-specific human rights frameworks focused on freedom of expression and privacy, such as the Global Network Initiative Principles and the Telecommunications Industry Dialogue Guiding Principles.

Sources:

- "Guiding Principles on Business and Human Rights" (United Nations, 2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.
- "Principles," Global Network Initiative, https://globalnetworkinitiative.org/principles/index.php.
- "Guiding Principles," Telecommunications Industry Dialogue, http://www.telecomindustrydialogue.org/about/guiding-principles/.

Figure 3 | Governance Scores



Notably, Twitter and Apple—which are not GNI members—perform significantly worse in this category: Twitter, for example, had an average score of 30 percent, while Apple placed eighth among internet and mobile companies in this category, scoring just 17 percent. The only internet and mobile companies to perform worse than Apple in the Governance category were the Russian internet companies, Mail.Ru and Yandex, and the Chinese internet companies, Tencent and Baidu.

Of the telecommunications companies, the highest scores in the Governance category went to TID members Vodafone, Orange, AT&T, and Telefónica. As with the internet and mobile companies, there was a sizable gap between companies that are members of the organization committed to implementation of freedom of expression and privacy principles and those that are not TID members.

Despite higher overall scores by GNI and TID members in the Governance category, one indicator in this category did not correlate to GNI or TID membership. Companies with better disclosure of grievance and remedy mechanisms, measured by Indicator G6, were not members of the GNI or the TID. Of the top five ranked companies, only one—Vodafone—is a TID member. Instead, higher scores on G6 tended to correlate roughly with the extent to which companies are required by law in their home countries to offer grievance mechanisms. One of the highest-scoring telecommunications companies was Bharti Airtel, and the highest-scoring internet and mobile company was Kakao.

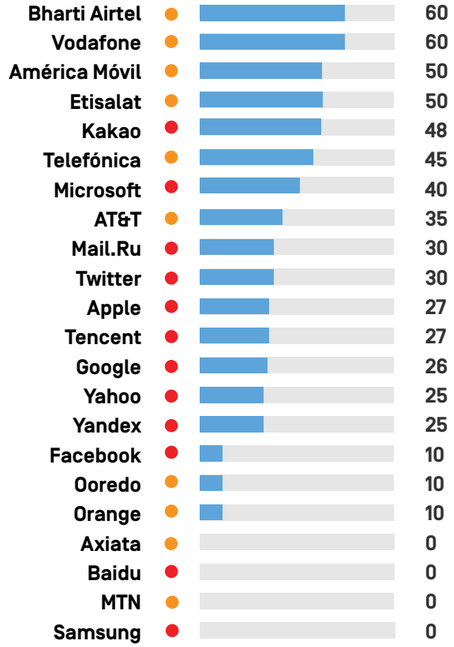
In order for people to use such mechanisms appropriately and effectively, companies need to provide users with sufficient information not only about how companies receive and handle government requests, but also about how companies handle private (non-government)

What Are Grievance and Remedy Mechanisms?

According to the U.N. Guiding Principles on Business and Human Rights, companies should establish a means of identifying and addressing any human rights violations or concerns that occur in relation to the company's business. Internet and telecommunications companies should demonstrate that they have clear mechanisms in place for people to file grievances and receive remedy. Similarly, users must also have a way of learning about these mechanisms.

Source: "Guiding Principles on Business and Human Rights," (United Nations, 2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Figure 4 | Disclosure of Grievance and Remedy Mechanisms (G6)



requests, how they collect, use, and share user information, and how companies enforce their own rules. This is one of many reasons why the Index places such great emphasis on transparency and disclosure.

3.5 Recommendations for Companies

- **Communicate with users in a clear, accessible, and organized way.** Companies should disclose and explain how they comply with laws and what that compliance means for users. Companies that are serious about demonstrating respect for users' rights should strive for well-organized disclosures in places that users can reasonably be expected to find. Users should not have to depend on external sources or be specialists in telecommunications or privacy law in order to learn about the company's commitments and practices.

- **Disclose evidence that the company has institutionalized its commitments.** It is great for a company to have leaders with strong personal commitments to users' rights, who make strong statements in speeches and the media. However, long-term respect for users' rights requires that such commitments are clearly institutionalized. This bolsters external confidence that the company's implementation of commitments and principles does not depend on specific individuals remaining employed by the company.

- **Conduct regular assessments to determine the impact of the company's products, services, and business operations on users' freedom of expression and privacy.** Several companies in the Index conduct different types of human rights impact assessments (HRIAs), a systematic approach to due diligence that enables companies to identify risks to users' freedom of expression and privacy as well as to enhance users' enjoyment of those rights. While it may be counterproductive for companies to publish all details of their processes and findings, it is important to disclose information about the fact that the company conducts assessments and basic information about the scope, frequency, and use of these assessments. For such disclosures to be credible, companies' assessments should be assured by an external third party that is accredited by an independent body whose own governance structure demonstrates strong commitment and accountability to human rights principles. As of 2017, only the Global Network Initiative meets the requirements for such an accrediting organization.

- **Publish transparency reports** including the volume, nature, and legal basis of requests made by governments and other third parties to access user information or restrict speech. Disclosures should include information about

the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own terms of service.[27]

- **Commit to push back against excessively broad or extra-legal requests, including in a court of law** while complying with bona fide requests to restrict speech or share user information within the bounds of the law. Companies should use every opportunity available to pressure governments to move away from mass surveillance and institute meaningful oversight over national security and law enforcement authorities.

- **Make clear to users what types of requests the company will—and will not—consider, from what types of parties.** For example: some companies make clear that they will only accept government requests for user information via specified channels and that they will not respond to private requests. Other companies do not disclose any information about whether they may consider private requests. Without clear policy disclosure about the types of requests the company is willing to entertain, users will lack sufficient information about risks that they may take when using a service.

- **Establish effective grievance and remedy mechanisms.** Grievance mechanisms and remedy processes should be more prominently available to users. Companies should more clearly indicate that they accept concerns related to potential or actual violations of freedom of expression and privacy as part of these processes. Beyond this, disclosure pertaining to how complaints are processed, along with reporting on complaints and outcomes, would add considerable support to stakeholder perception that the mechanisms follow strong procedural principles and that the company takes its grievance and remedy mechanisms seriously.

4. MOBILE ECOSYSTEMS: WE DON'T KNOW ENOUGH ABOUT THE IMPACT OF SMARTPHONES ON OUR DIGITAL RIGHTS

All three mobile ecosystems evaluated—Apple iOS, Google Android, and Samsung's implementation of Android—offered poor disclosure about policies affecting freedom of expression and privacy.

Most people today access the internet via mobile devices, particularly with the miniature computers known as "smartphones." Through these mobile devices, users can access data stored on remote servers, navigate with GPS-enabled maps, photograph their daily lives, read the news, and connect with family, friends, and colleagues around the globe.

But smartphones are also tracking devices that leave a digital trace of our every movement, both online and offline. Companies that produce these devices are the custodians of sensitive user information, as well as gatekeepers to countless types of apps available in their app stores—and therefore have tremendous influence over users' freedom of expression and privacy.

What Do We Mean by "Mobile Ecosystems"?

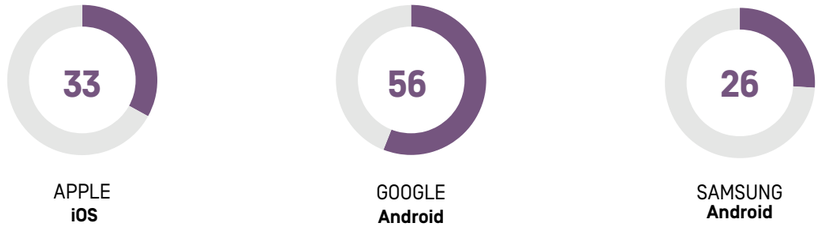
The Index defines mobile ecosystems as: "the indivisible set of goods and services offered by a mobile device company, comprising the device hardware, operating system, app store, and user account."

Read our full analysis of mobile ecosystems at: https://rankingdigitalrights.org/index2017/findings/mobileecosystems.

Sources:

- "2017 Indicators: Glossary," Ranking Digital Rights, https://rankingdigitalrights.org/2017-indicators/#Glossary.
- Nathalie Maréchal, "What Do We Mean by Mobile Ecosystems?" Ranking Digital Rights, September 15, 2016, https://rankingdigitalrights.org/2016/09/15/what-are-mobile-ecosystems/.

Figure 5 | Mobile Ecosystems: Overall Scores



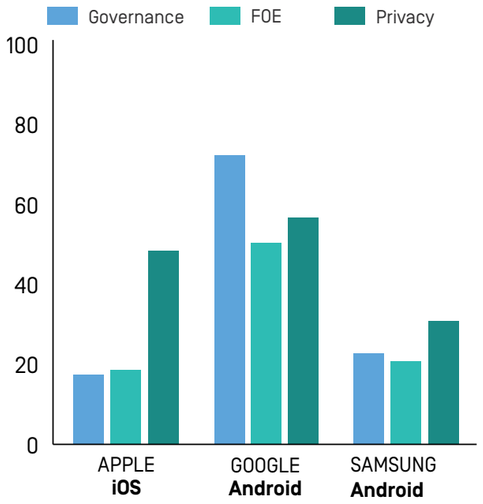
For this reason, the 2017 Index was expanded to include Apple iOS, Google Android, and Samsung's implementation of Android—makers of mobile devices and software products that we call "mobile ecosystems."

All three mobile ecosystems evaluated failed to sufficiently disclose policies affecting users' freedom of expression and privacy. This means that it is difficult for users to know and understand how their Apple or Android smartphones control their ability to create, share, and access content, or how mobile ecosystem companies determine who has access to their information under what circumstances.

While all companies fall short, Google's Android had stronger disclosure of policies pertaining to users' freedom of expression and privacy than Apple's iOS or Samsung's implementation of Android. The starkest differences were in the Governance and Freedom of Expression categories—in both categories, Google led both Apple and Samsung by a wide margin. Google made stronger commitments to protect users' freedom of expression rights at the company-wide level and provided stronger disclosure of policies that affect these rights for Android users.

Apple, by contrast, disclosed a commitment to protect users' privacy at the company level but made no such commitment to protect freedom of expression—and had similarly weak disclosure of policies that affect freedom of expression for iOS users. Samsung's level of disclosure was similar. The South Korean company makes prominent commitments to human rights, privacy, and freedom of expression at the corporate level but does not sufficiently disclose how or whether those commitments are implemented in practice.

Figure 6 | Mobile Ecosystems: Scores by Index Category



4.1 Chokepoints for Expression

The Apple App Store, Google Play Store, and Samsung Galaxy Apps store are chokepoints for freedom of expression.

All three mobile ecosystems failed to sufficiently disclose policies affecting users' freedom of expression. While Google's Android disclosed far more than its peers, no company provided enough information to enable app users and app developers to fully understand what kinds of content can be created and shared, what types of activities are prohibited, or the consequences for violating these rules.[28] For all companies, the terms of service agreements for app users and app developers were neither easy to find nor to understand (F1).[29] None provided any data about the volume of content or accounts they restrict for terms of service violations (F4),[30] and only Google provided some disclosure of whether it notifies app developers when it removes an app for breaching Play Store rules (F8).[31]

Apple iOS revealed little about how it handles government and private requests to remove content, specifying only that a court order would be required (F5). Samsung provided no information about how it responds to such requests. Google—an industry leader in transparency reporting—disclosed considerably more. Unlike Apple and Samsung, Google's transparency report disclosed the number of government requests it received to remove third-party apps from its Play Store (F6).[32]

All three companies disclosed a policy of requiring app developers to verify their identities as a condition of registering with their app developer programs (see page 30 for more on companies' identity policies).

4.2 Gatekeepers for Privacy and Security

All three mobile ecosystems evaluated are weak gatekeepers for user privacy on their app stores.

While Apple, Google, and Samsung each disclosed they require apps that collect user information to provide a privacy policy (P1), none disclosed that they review privacy policies of apps in a way that provides adequate privacy safeguards for users.

Why Security Updates Matter

Given the vast amounts of sensitive personal information saved on and generated by smartphones, users' freedom of expression and privacy relies on the devices' software being up-to-date and resilient against malware. The timely delivery of software updates to mobile devices is a major security and equity issue worldwide. Indeed, the newest and most expensive smartphones are more likely to be up-to-date than older, inexpensive models, leaving lower-income users more vulnerable to malware and targeted hacking.

Android models from the Nexus and Pixel product lines and iOS devices receive updates directly from Google and Apple, respectively, but other Android devices—including those made by Samsung—often lag weeks or months behind. Manufacturers and telecommunications companies alike can modify Android's code for various reasons, and this in turn affects how quickly users receive updates after they are released by Google. As a result, users can spend months using unpatched devices with known vulnerabilities. It is therefore critical for companies to deliver security updates to users within 30 days of the patch being made available, and to clearly communicate to users for how long after purchase (or until what date) they are guaranteed to receive software updates.

Third-party apps often collect large amounts of data without adequately informing users or obtaining their consent, including information that is overly broad or irrelevant to the app's function—for example, ride-sharing apps that require constant access to geolocation or games demanding access to users' contacts (P3).

Lack of security updates leaves users exposed. Google was the only company to disclose how long various device models would be guaranteed to receive software updates—a "best by" date for smartphones. Apple and Samsung did not provide such information, making it difficult for users to evaluate for how long their devices will be safe to use (P14).[33]

4.3 Recommendations for Companies

- **Recognize app store content as a freedom of expression issue.** Companies that have committed to freedom of expression principles should ensure that mobile ecosystems and app stores are clearly covered by due diligence and governance processes necessary to implement those principles.
- **Clearly disclose policies and processes for handling requests to remove or pre-emptively restrict apps**, whether such requests come from governments or from other entities. Companies should also disclose in their transparency reports information about app removals and restrictions from their app store, including the number of requests received and complied with as well as data about apps or other content removed in the process of terms of service enforcement.
- **Commit to enforce app store terms of service that require all apps collecting user information to have a privacy policy**. Commit to evaluate the content of those privacy policies, and disclose information about this enforcement process in transparency reports.
- **Commit to deliver all security updates to users within 30 days** of a patch being made available. Companies should also clearly communicate to users for how long after purchase (or until what date) they should expect to receive software updates.

5. FREEDOM OF EXPRESSION IS GETTING SHORT-CHANGED

With a couple of notable exceptions, companies on average disclosed the least amount of information about policies that affect users' freedom of expression.

Digital technologies have revolutionized how people communicate, giving billions of people unprecedented access to global information flows. Yet freedom of expression is under siege. Freedom House reports a steady 10-year decline in freedom around the world, with some of the sharpest declines in freedom of expression.[34]

Different governments all over the world approach online expression with varying degrees of commitment to freedom of expression as a universal human right. In more authoritarian countries, governments have steadily expanded laws that restrict speech online, and have resorted to blocking entire platforms and applications or shutting down communications networks altogether when more targeted censorship efforts fail.[35] Even in countries with stronger commitment to freedom of expression, democratically elected governments have sought to compel companies that host user-generated content to limit certain types of speech that many of their citizens believe is harmful.[36] Yet while companies have improved their transparency in recent years regarding government demands for user information, there is still not enough clarity around how companies respond to requests to censor content, restrict accounts, or shut down communications networks.

In addition to government-imposed requirements, companies also make choices that determine if and how people are able to exercise their freedom of expression rights. For example, telecommunications companies' policies regarding network management may favor certain types of content or services over others, while most companies that host user-generated content have rules about what types of content or activities are prohibited on their platforms, beyond what is restricted by law.

The 2017 Index uses 11 indicators to measure if and how clearly companies disclose policies that affect users' freedom of expression, thereby evaluating whether they respect the right to freedom of expression of users, as articulated in international human rights instruments.[37] A company should disclose how it works to avoid contributing to actions that may interfere with this human right, except where such actions are lawful, proportionate

and for a justifiable purpose. For example, companies may block users from publicly sharing content that is copyrighted, depicts the sexual abuse of children, or incites violence against groups of people.

5.1 Insufficient Disclosure

Companies don't tell us enough about how they respond when governments and other parties ask them to block, delete, or otherwise restrict content or restrict users' accounts.

Companies increasingly receive requests to remove, filter, or restrict access to content or to suspend users' accounts. These requests come from governments, courts, and private organizations and individuals. Requests to remove content can pertain to copyright infringement, hate speech, child sex abuse images, and pornography, as well as speech that is deemed critical of governments or officials, or that may violate national security laws.

If and how companies respond to and comply with these requests can have a critical impact on freedom of expression and on human rights more broadly.

> **We expect companies to publicly disclose their processes for responding to requests by governments and private parties to remove content or suspend a user's account.**

Civil society organizations, journalists, political opposition groups, religious minorities, and many other types of people whose speech and communication is most vulnerable to suppression depend on a range of digital tools and platforms to communicate ideas and information. We therefore expect companies to publicly disclose their processes for responding to requests by governments and private parties to remove content or suspend a user's account. We also expect them to comply with requests that affect users' speech, communication, and access to information only when there is a legal reason for doing so, and to investigate and push back on requests that are unlawful or overbroad.

Despite positive trends, our data showed that few companies provided enough information for users to be able to understand how companies respond to requests from governments and private parties to take actions that affect users' freedom of expression. Even companies with the most disclosure could do far more to explain both how they respond to and whether they comply with such requests.

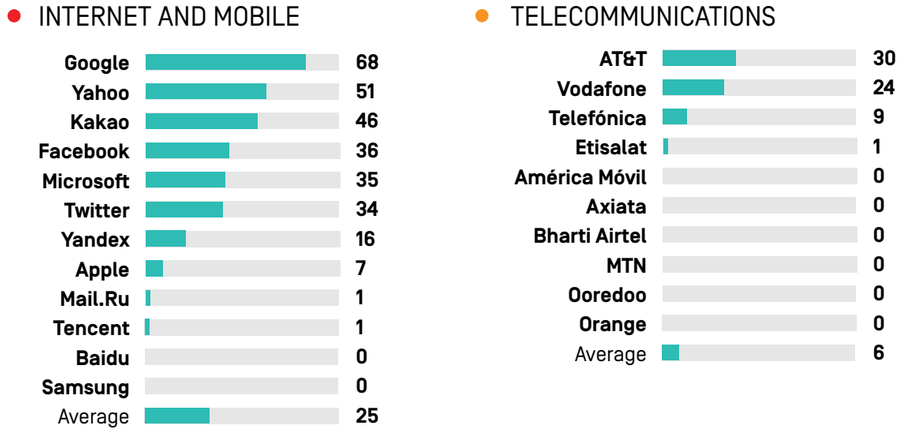
What Do We Mean by "Private" Requests?

Private requests are requests made by any person or entity that is not acting under direct governmental or court authority. Many private requests are made as part of processes sanctioned or stipulated by copyright and child protection laws. Private requests for content restriction can come from a notice-and-takedown system, such as the U.S. Digital Millennium Copyright Act, or from a self-regulatory body, such as the Internet Watch Foundation.

Sources:

- "2017 Indicators: Glossary," Ranking Digital Rights, https://rankingdigitalrights.org/2017-indicators/#Glossary.
- For more information on notice-and-takedown, as well as the DMCA, see Rebecca MacKinnon et al., "Fostering Freedom Online: The Role of Internet Intermediaries," (UNESCO, 2014), http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Figure 7 | Disclosure of Government and Private Requests to Restrict Content and Accounts (F5-F7)



- Companies tended to reveal more about their process for responding to government and private requests (F5) than they did about the actual number and type of government and private requests they received and with which they complied (F6, F7).

- Few companies reported any information about the number of private requests they received to remove content (F7).

- Internet and mobile companies on average tended to disclose far more information than telecommunications companies: of the 10 telecommunications companies evaluated in the 2017 Index, only four provided some information about how they handle government and private requests (see Figure 7).

- Companies should clarify their policies regarding private requests, particularly if they only respond to private requests they receive through court orders. For example, while Vodafone disclosed that it responds to requests from some private entities such as the Internet Watch Foundation, it did not state whether it responds to any other private requests. AT&T, on the other hand, clearly stated that it does not respond to any private requests apart from subpoenas it receives from civil proceedings.

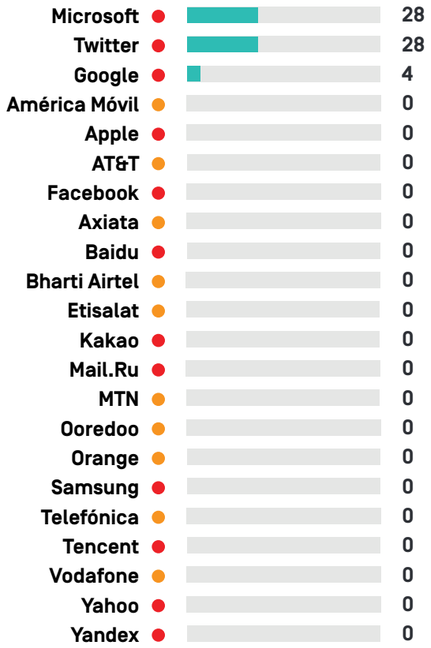
5.2 Terms of Service Enforcement

Companies tell us almost nothing about when they remove content or restrict users' accounts for violating their rules.

Companies also take actions that affect users' freedom of expression for reasons unrelated to government or private requests. Through their terms of service and user agreements, companies set their own rules for what types of content or activities are prohibited on their services and platforms. They also have their own internal systems and processes for enforcing these rules. Measures can include deleting content, restricting a user's access to the service, or shutting down accounts altogether.

Companies are expected to have rules about what types of content and activities are forbidden. There are legitimate reasons to restrict speech, as discussed above. However, transparency and accountability are essential. Without any insight into how companies implement their own terms of

Figure 8 | Disclosure of Data on Terms of Service Enforcement (F4)



service and other key policies, the public has no ability to understand if and how a company's actions affect their freedom of expression and access to information. Companies must be accountable to ensure that their enforcement policies do not end up being abused in a manner that silences legitimate speech, including activism, journalism, or debates about controversial social, political, or religious issues.

The 2017 Index contains one indicator (F4) addressing whether companies disclose the volume and nature of content and accounts they restrict for terms of service violations.[38] The indicator measures if the company publishes data on these activities regularly and makes this data available in a structured, downloadable format.

Our research showed that companies are starting to move in the right direction: while no company provided any disclosure on this indicator in the 2015 Index, this year three companies—Microsoft, Twitter, and Google—received credit for disclosing some data about content they remove for terms of service violations.

Twitter: In a blog post from February 2016, Twitter disclosed that since the middle of 2015, the company had suspended over 125,000 accounts for "threatening or promoting terrorist acts."[39] In a follow-up post six months later, Twitter announced it had suspended an additional 235,000 accounts.[40]

Microsoft: Microsoft's Transparency Hub, launched in October 2015, disclosed data about its removal of "non-consensual pornography" in breach of its terms of service.[41] However, the company did not publish data on any other types content it may have removed for terms of service violations.

Google: Google received a few points for disclosing data about content removals on YouTube. In a blog post from September 2016,[42] YouTube stated that in 2015 the company removed 92 million videos for violating its terms of service. It also reported that one percent of the videos it removed were for hate speech and terrorist content.

5.3 Identity Policies

Identity policies tied to government ID threaten freedom of expression.

The ability to communicate anonymously is essential to freedom of expression. In 2015, U.N. Special Rapporteur David Kaye issued a report affirming that anonymity enables freedom of expression and opinion in the digital age.[43]

It is not uncommon in more restrictive environments like China, Iran, and Russia for governments to require internet service providers to keep records of users' identities as a means of tracking and cracking down on human rights defenders and political dissent. Democratic governments also can and often do require internet and telecommunications companies to document and verify the identities of users to assist with law enforcement and counterterrorism efforts. A growing number of governments have for instance introduced mandatory registration of pre-paid SIM card users in recent years for these reasons.[44] However, mandatory identification requirements can pose serious threats to users' right to freedom of expression, especially in jurisdictions where governments can easily demand or otherwise gain access to user information held by companies.

The 2017 Index has one indicator (F11, "Identity policy") measuring if companies clearly disclose whether they require users to verify their identity with a government-issued identification or another form of identification that could be connected to their offline identity.[45] This indicator applies to internet and mobile companies, as well as to pre-paid mobile services for telecommunications companies.

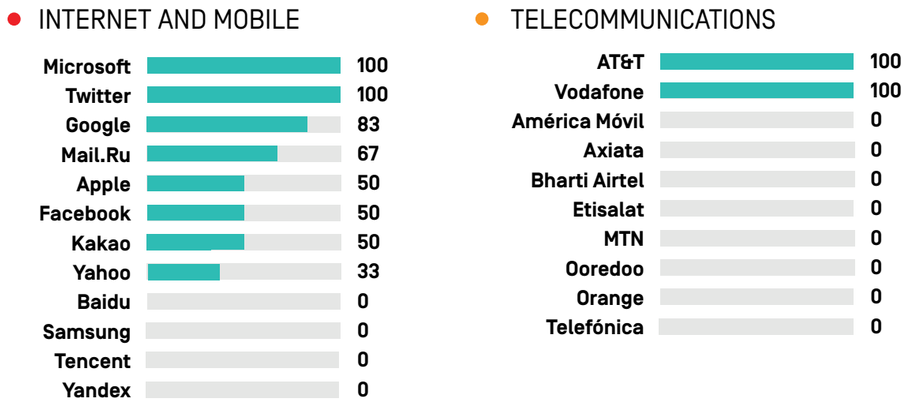
Of the 22 companies evaluated, 18 disclosed a policy of requiring users to verify their identity as a condition of using at least one the company's services evaluated.

- Twitter had one of the better examples of a clearly disclosed identity policy that explicitly states: "Twitter doesn't require real name use, email verification, or identity authentication."[46]

- Although Google disclosed it does not require users to verify their identity for Gmail, YouTube and Google Play, it lost points for requiring Google Play app developers to do so by making a small credit card transaction. This policy is a barrier to someone who might want to develop an app but who, for example, lives under an authoritarian government with a history of censoring apps or going after individuals who express dissent online.

- Yahoo also lost points on identity policies for Yahoo Mail and Flickr. Yahoo disclosed that it requires users to provide a phone number when creating an account, which in some jurisdictions can be used to connect a user with their offline identity.

Figure 9 | Identity Policies (F11)



- Orange (France) requires pre-paid mobile users to verify their identification although there is no explicit legal requirement in France to do so.

5.4 Network Shutdowns

Users are in the dark about why they're cut off.

Network shutdowns are a growing threat to human rights around the world. In a resolution passed in June 2016, the U.N. Human Rights Council affirmed that network shutdowns threaten freedom of expression and the right to access information, condemned them as a violation of international human rights law and called on governments to refrain from taking these actions.[47] Yet governments are increasingly ordering telecommunications companies to shut down their networks,[48] which in turn puts pressure on companies to take actions that violate their responsibility to respect human rights.

As the Internet Society puts it:

> **"We understand that governments are faced with sometimes challenging situations that may threaten public order and national security. But we do not believe that shutting down communications for whole or part of a country is an appropriate and proportional measure. We encourage governments to look at alternative means to address such issues."[49]**

While companies do not control government actions or the laws that justify and enable governments to demand network shutdowns, companies have a responsibility to disclose what actions they are taking, and under whose authority, so that those responsible can be appropriately held accountable. In fulfilling their responsibility to respect human rights, companies also have an obligation to do everything possible to minimize human rights harms that may result from compliance with government shutdown orders, by minimizing the scope and extent of compliance and by avoiding compliance with orders of dubious legality.

In response to growing concern by a range of stakeholders—from human rights groups to investors—we created a new indicator for the 2017 Index focused specifically on network shutdowns (F10). It reads:

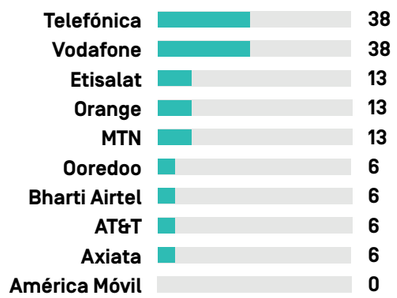
> **"The company should clearly explain the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network."[50]**

All telecommunications companies evaluated failed to meet this obligation to varying extents; however, Telefónica and Vodafone stood above the rest by disclosing the most information about their policies for responding to network shutdown orders.

Notably, while Telefónica and Vodafone disclosed the most information about shutdowns, they disclosed different things: Telefónica disclosed more information about the number of requests it receives and the legal authority behind such requests, while Vodafone committed to push back against network shutdown requests.

The two companies with the highest disclosure about shutdowns, Telefónica and Vodafone, are both members of the Telecommunications Industry Dialogue (TID), whose members commit to respect freedom of expression and privacy. However, the two other TID members, Orange and AT&T, disclosed no more information about network shutdowns than the lowest-scoring companies in the Index.

Figure 10 | Disclosure of Network Shutdown Policies (F10)



5.5 Recommendations for Companies

- **Improve transparency and accountability about all types of third-party requests to restrict content or user accounts—made by governments as well as by private individuals and organizations.** To the maximum extent possible under the law, companies should publish comprehensive information (including transparency reports) related to the following types of third-party requests:
  - Process for responding to all types of third-party requests to restrict content, access, or service;
  - Data about government requests to restrict content, access, or service;
  - Data about private requests for content restriction. If a company does not receive or entertain a particular type of request, or if it doesn't entertain requests from certain types of third parties (e.g., private individuals acting without legal authority), the company should also clearly disclose that information.
- **Telecommunications companies should provide as much information as possible about their policies for responding to network shutdowns**, including details such as the number of requests they received and the number with which they complied.
- **Companies that host or serve as a conduit for content should disclose sufficient detail to meet standards for transparency and accountability around terms of service enforcement.** Specifically, companies should publish data on a regular basis about the volume and nature of content removals and account restrictions that the company makes to enforce its terms of service so that users have a clearer understanding of the level of effort the company is making to keep different types of speech from appearing on or through its service.
- **Where the law does not explicitly mandate it, refrain from requiring users to register their identity**, such as by providing a government-issued document or a credit card (other than for billing purposes, if applicable).

Companies have an obligation to minimize human rights harms that may result from compliance with government shutdown orders, by minimizing the scope and extent of compliance and by avoiding compliance with orders of dubious legality.

6. HANDLING OF USER INFORMATION: WE ARE STILL IN THE DARK

We are still in the dark about everything companies know about us and how our information is used. Companies continue to fail to provide users with adequate information about how and for what purpose their information is collected, shared, retained, and used.

If somebody wanted to build a profile on you based on all the information companies hold about you, what would it look like? At current levels of disclosure among the companies evaluated in this Index, we remain no closer to being able to answer that question than we were in 2015.

While some companies disclosed more than others, none disclosed enough detail about their policies for handling user information for people to fully understand the privacy implications of signing up for a service. They also gave users insufficient options to control what information is collected and shared with third parties, and few offered options for users to obtain all the information that the company holds about them.

The 2017 Index contains seven indicators measuring if and how clearly companies disclose what types of user information they collect, share, for what purpose, how they collect this information, and for how long they retain it. Indicators also look for companies to offer users options to control what is collected and to obtain all of the information a company holds on them.

User Information: How the Index Defines It

By "user information" we mean any information that identifies a user's activities, including personal correspondence, user-generated content, account preferences and settings, log and access data, data about a user's activities or preferences collected from third parties, and all forms of metadata.

Source: "2017 Indicators: Glossary," Ranking Digital Rights, https://rankingdigitalrights.org/2017-indicators/#userinformation.

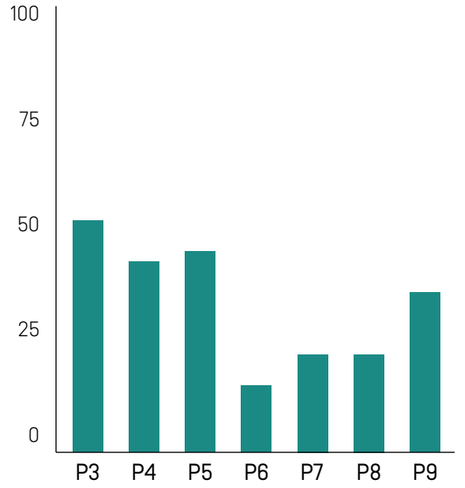
34

6.1 Who, What, How, Why?

Our research showed that while companies generally lacked transparency about how they handle user information, they tended to disclose slightly more about what they collect and for what purpose (P3, P5) than about what information they share (P4) and for how long they retain it (P6).

Few companies offered disclosure about whether users can control what user information the company collects or how their information is used for targeted advertising (P7). Companies also lacked disclosure about whether users could obtain all public-facing and private user information a company holds about them (P8).

Figure 11 | Disclosure of Handling of User Information: Average Scores (P3-P9)



P3 Collection of User Information
P4 Sharing of User Information
P5 Purpose for Collecting and Sharing User Information
P6 Retention of User Information
P7 Users' Control Over Their Own User Information
P8 Users' Access to Their Own User Information
P9 Collection of User Information From Third Parties (Internet and mobile companies)

Internet and mobile companies did not adequately disclose what information is collected about users from third parties (P9). Some companies continue to collect information about a user even when the user is on a different website or app, typically through the use of cookies, plug-ins, widgets, and ad-tracking services. Company disclosure of these practices helps users understand if and how their activities are being tracked even when they are not on a particular company's website or app. Our data showed that few companies disclosed sufficient information about these practices.

Internet and mobile companies revealed more than telecommunications companies—but still not enough.

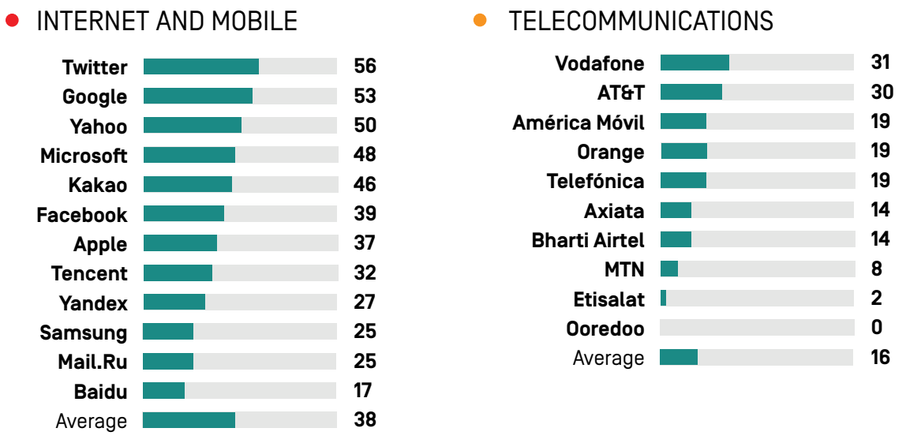
Internet and mobile companies, on average, disclosed more about how they handle user information, outscoring telecommunications companies by 22 percentage points (see Figure 12). Even so, the average score among internet and mobile ecosystem companies was just 38 percent, with a majority of companies providing only minimal disclosure.

Among internet and mobile companies, Twitter had the highest average score, followed by Google, Yahoo, Microsoft, and Kakao.

Twitter's privacy policy was one of the more clear examples of a company explaining how it handles each type of information it collects.[51] Still, the company did not commit to limit collection of user information to only what is necessary for the service (P3),[52] and did not fully disclose what information it shares with third parties (P4).[53]

Telecommunications companies, on average, disclosed far less than internet and mobile ecosystem companies (see Figure 12). While Vodafone and AT&T disclosed more than their peers, telecommunications companies in general

Figure 12 | Disclosure of Handling of User Information (P3-P9)



failed to provide sufficient information about all of the types of information they collect, share, and retain. Among these companies, AT&T was the only one to disclose any information about how long it retains the information about users that it collects (P6).[54] The overall low scores among telecommunications companies across these indicators highlights a troubling lack of transparency about how they handle user information.[55]

6.2 User Control

Users lack options to control what companies collect.

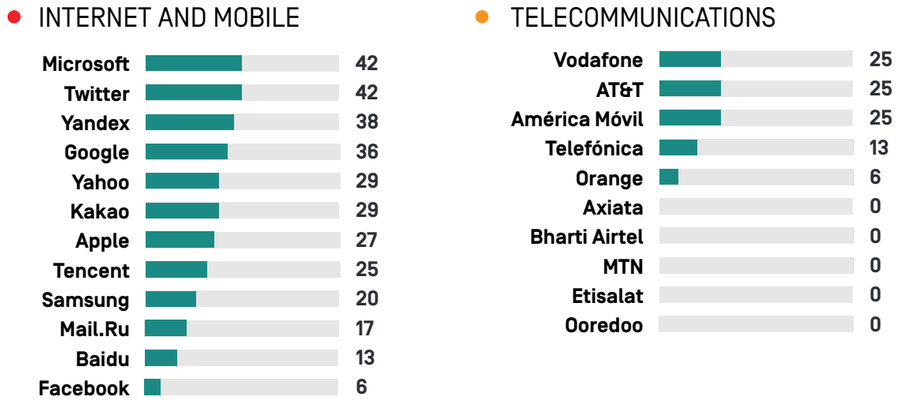
An example of inadequate disclosure can be found in the results for Indicator P7 (see Figure 13), which seeks disclosure from companies about what, if any, options users have to control the information that the company collects on them.[56]

Companies disclosed little. Among internet and mobile companies, Microsoft and Twitter provided the most information in comparison to their peers, although both still fell short. Microsoft disclosed options allowing users to control some information collected when they use the Bing search engine but not for Outlook or Skype. Twitter did not clearly disclose what options users have to control all of the types of information the company collects on them. Both companies gave options to control how information is used for targeted advertising, indicating that targeted advertising is on by default.

Facebook received the lowest score of all internet and mobile companies for its lack of disclosure about how users can control what the company does with their information. For Instagram and WhatsApp, the company offered some options about how and whether their information is used for targeted advertising. However, it did not clearly disclose what options users have to control the different types of information collected or whether users can delete the information that the company has collected on them.

Among telecommunications companies, Vodafone, AT&T, and América Móvil had the highest scores, although the average among the 10 telecommunications companies was just nine percent. Half of these companies received no credit whatsoever on this indicator.

Figure 13 | Disclosure of Options for Users to Control Their Information (P7)



Despite the EU's strong data protection laws, disclosure among EU companies varied significantly and none of the companies disclosed enough information on this indicator for users to understand their options for controlling their information. Of the three EU companies, Vodafone (UK) scored 25 percent, followed by Telefónica (Spain) with 13 percent, and Orange (France) with just six percent.

Vodafone, for example, provided users with options to control how their information is used for targeted advertising but did not disclose options to control what the company collects in the first place. Orange only disclosed that users can object to their personal data being used for targeted advertising, but this only applies to some of their information. While EU regulations may require that companies obtain consent around the collection or processing of data, it is also imperative that companies communicate these options clearly to users.

6.3 Recommendations for Companies

Provide users with a more comprehensive picture of the lifecycle of their personal information, from collection to use to sharing to retention and deletion.

Disclosures should include:

- What specific types of information the company collects (P3);
- How the company collects that information (e.g., does a company ask users to provide certain information, or does the company collect it automatically?) (P3);
- Whether users have an option not to provide that information (P7);
- Specifically, what information the company shares and with whom (P4);
- Why the company shares that information (P5);
- Whether—and the extent to which—users can control how their information is used (P7);
- How long the company retains that information (P6);
- Whether the user can access all public-facing and private user information a company holds about them (P8);
- Whether and how the company destroys that information when users delete their accounts or cancel their service (P6).

7. SECURITY COMMITMENTS LACK SUFFICIENT EVIDENCE

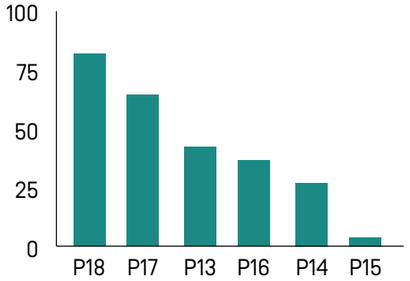
Companies do not communicate enough about their security policies and practices for users to trust that credible efforts are being made to secure their information.

People entrust companies with enormous amounts of personal information—and also expect companies to respect their privacy and protect their personal data. Privacy is broader than security, but without security there is no privacy.

For this reason, companies should clearly disclose if and how they secure users' information. In some cases, disclosing too many specifics about security practices can be counterproductive and leave companies and the data in their custody vulnerable to attackers. But it is reasonable to expect companies to reveal basic information that provides evidence they are adhering to industry best practices on security so that users know what steps are being taken to secure their privacy, and can decide whom to trust with their information accordingly.

The 2017 Index uses six indicators to measure if and how well companies disclose their policies and practices for securing user information. These indicators address both what companies disclose about their own internal security policies and practices as well as what tools and information they supply to users to help them protect themselves.

Figure 14 | Average Security Scores, by Indicator (P13-P18)



P18 Inform and Educate Users About Potential Threats

P17 Account Security (Internet and mobile companies)

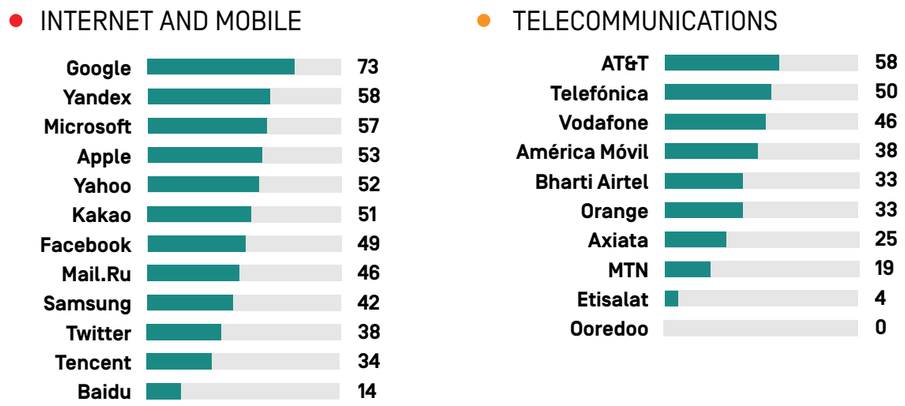
P13 Security Oversight

P16 Encryption of User Communication and Private Content (Internet and mobile companies)

P14 Addressing Security Vulnerabilities

P15 Data Breaches

Figure 15 | Disclosure of Security Policies (P13-P18)



2017 Index: Security Indicators

P13. Security Oversight: Does the company clearly disclose information about its internal processes to ensure the security of its products and services?

P14. Addressing Security Vulnerabilities: Does the company address security vulnerabilities when they are discovered? Does it disclose a bug bounty program that allows independent researchers to submit security vulnerabilities they discover?

P15. Data Breaches: Does the company publicly disclose information about its processes for responding to data breaches?

P16. Encryption of User Communication and Private Content (Internet and mobile companies): Does the company disclose it encrypts user communication and private content so users can control who has access to it?

P17. Account Security (Internet and mobile companies): Does the company disclose what users can do to keep their accounts secure?

P18. Inform and Educate Users About Potential Threats: Does the company publish practical materials that educate users on how to protect themselves from cyber risks relevant to their products or services?

7.1 Communication Gaps

Companies communicate less about what they are doing to protect users' security than they do about what users should do to protect themselves.

This is demonstrated by the notably high scores on Indicators P17 and P18, asking how companies inform users about what they can do to keep their own accounts secure (Figure 14). High scores on those two indicators contrasted with markedly lower scores on indicators that measure if and how companies disclose their own internal processes for securing user information (P13, P14, P15, P16).

Among the internet and mobile companies, Google earned the highest marks on this set of indicators, with a 15-percentage point lead over the second-ranked company, Yandex, followed by Microsoft, Apple, Yahoo, and Kakao (Figure 15).

AT&T led the telecommunications companies on these indicators, followed by Telefónica and Vodafone. AT&T was the only telecommunications company to receive full credit for its disclosure of internal security practices that include limiting employee access to user data and conducting internal and external security audits (P13).

7. 2 Data Breaches

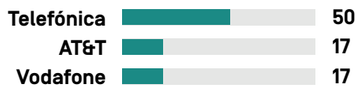
Only three companies—Telefónica, AT&T, and Vodafone—disclosed any information about their process for responding to data breaches.

Data breaches continue to make headlines and threaten the security and privacy of people's digital communications and sensitive personal data, like passwords, social security numbers, and financial information. In 2016 the number of data breaches in the U.S. alone was reported to have increased by 40 percent.[57] The Internet Society, concerned about the extent to which data breaches are eroding public trust in the internet, recently warned that "stakeholders do not have full information about the risks they may face online, making it difficult to take informed decisions."[58]

In response to such mounting concerns, the 2017 Index included a new indicator to measure if and how companies disclose their processes for responding to breaches (P15).[59] Many jurisdictions have laws in place requiring companies to notify designated authorities and affected users, within varying time frames depending on the nature of the breach. In their public disclosure, companies should state that their process involves these notification steps. In describing their process for addressing the impact of the data breach, companies should also disclose what kinds of services they may provide to affected users.

Only three companies—Telefónica, AT&T, and Vodafone—disclosed any information about their process for responding to data breaches, but even these companies disclosed very little. Telefónica received the most credit for disclosing its process for notifying users who may be affected by a data breach, and committing to inform customers about the steps it is taking and that users can take to mitigate the impact of a data breach. AT&T and Vodafone both received the same score on this indicator. AT&T was credited for committing to notify users in case of a data breach in accordance with laws and regulations. Vodafone received some credit for disclosing that it has a program in place to address the impact of a data breach, but did not provide enough detail about the specific steps it commits to take to address the impact.

Figure 16 | Data Breaches (P15)



7.3 Encryption

Encryption is important to protect users—but companies do not consistently disclose that they are protecting users with the highest level of encryption available, nor do they explain what barriers prevent them from doing so.

In a connected world in which basic human rights are under threat from all quarters, encryption is one of the more meaningful tools available to protect freedom of expression and privacy. The U.N. Special Rapporteur on Freedom of Expression has stated unequivocally that encryption and anonymity are essential for the exercise and protection of human rights.[60]

Yet encryption is a hot-button political issue around the world. In April 2016 a bill was introduced in the U.S. Senate that would require companies to provide authorities with search warrants access to encrypted data.[61] The French government has also signaled a desire to institute similar requirements.[62]

In Russia, laws enacted in 2016 require all ICT companies to provide authorities with decryption keys upon request, effectively banning end-to-end encryption.[63] While purportedly intended to assist authorities in criminal investigations, the Russian law criminalizes activities that are protected under international human rights frameworks. The weakening of encryption in Russia thus exposes journalists, human rights activists, political dissidents, and ordinary users to state surveillance outside of any meaningful oversight.

> **Encryption is important to protect users, but companies do not consistently disclose that they are protecting users with the highest level of encryption available, nor do they explain what barriers prevent them from doing so.**

Encryption hides the content of communications so only the intended recipient can view it. The process uses an algorithm to convert the message into a coded format so that the message looks like a random series of characters. Only someone with the appropriate decryption key can read the message. Data can be encrypted at different points: when it is in transit and when it is stored ("at rest").

Forward secrecy is an encryption method notably used in HTTPS web traffic and in messaging apps, in which a new key pair is generated for each session (HTTPS), or for each message exchanged between the parties (messaging apps). This way, if an adversary obtains one decryption key, they will not be able to decrypt past or future transmissions or messages in the conversation.

Forward secrecy is distinct from **end-to-end encryption**, which ensures that only the sender and intended recipient can read the content of the encrypted communications. Third parties, including the company, would not be able to decode the content. Many companies only encrypt traffic between users' devices and the company servers, maintaining the ability to read communications content. They can then serve targeted advertising based on users' data and share user information with the authorities.

Sources:

- "2017 Indicators: Glossary," Ranking Digital Rights, https://rankingdigitalrights.org/2017-indicators/#endtoend.
- "What Is Encryption?" Surveillance Self-Defense, April 22, 2015, https://ssd.eff.org/en/module/what-encryption for more information on encryption.

There are different kinds of encryption depending on the security objective and the type of product or service. For example, end-to-end encryption, which prevents even the company from reading user communications, is an important feature for email and messaging services, but not for content that is shared publicly on social networks. On the other hand, encryption in transit (which protects internet traffic from attackers) is essential for all services, but in practice is implemented differently from one service to another.

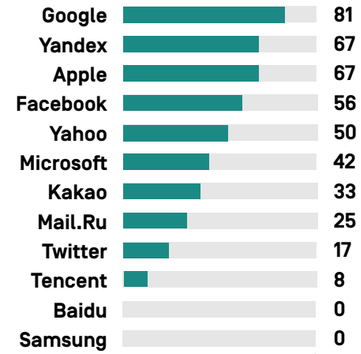
The 2017 Index includes one indicator (P16) that measures disclosure by internet and mobile ecosystem companies of their encryption policies.[64] Four elements measure whether and how clearly companies disclose if:

- the transmission of user communications is encrypted by default;
- the transmissions of user communications are encrypted using a unique key (what is referred to as "forward secrecy");
- users can secure their private content using end-to-end encryption (meaning not even the company can access the content);
- end-to-end encryption is enabled by default.

Among the 12 internet and mobile companies evaluated, Google overall disclosed the most about its encryption policies, followed by Apple, which scored on par with the Russian internet company Yandex (Figure 17).

This is likely to come as a surprise to many, given Apple's reputation for strong security and its recent legal skirmishes with the U.S. Federal Bureau of Investigation over end-to-end encryption.[65] But Google's disclosures were consistently clearer and more thorough than Apple's, while Yandex was remarkably forthcoming about its practices, especially compared with the other Russian company in the Index, Mail.Ru, which hardly disclosed any information about its encryption policies.

Figure 17 | Disclosure of Encryption Policies (P16)



But even for Google and Apple, there is much room for improvement. For instance, Google does not offer end-to-end encryption in Gmail. Apple failed to disclose whether iMessage communications are encrypted with unique keys, or what is referred to as "forward secrecy."

Meanwhile, Twitter had one of the lowest scores of all internet and mobile companies, particularly compared to its U.S. peers. The company revealed that for Twitter's flagship platform, users' internet traffic between their device and the company's servers is encrypted by default, and with forward secrecy. However, the company provided no similar information for its Vine and Periscope services, nor did it provide end-to-end encryption for direct messages or clearly disclose that the content of such messages is not secure.

7.4 Recommendations for Companies

- **Disclose clear information about policies for addressing security vulnerabilities**. This disclosure should include bug bounty programs and the company's practices for relaying security updates to mobile phones.
- **Disclose processes for mitigating the risk and severity of data breaches.** Companies should also disclose procedures for dealing with breaches when they occur. Companies should communicate with users and provide them with an appropriate remedy.
- **Where permitted by law, publicly commit to implement the highest encryption standards available.** This disclosure should include encryption in transit, end-to-end encryption, and forward secrecy. At minimum, make it possible for users to encrypt their own data as securely as possible and communicate this to users clearly. Where the law prohibits strong encryption, clearly say so to users, explaining the specific legal barrier and the potential consequences for user privacy and safety.

8. RECOMMENDATIONS FOR GOVERNMENTS

- **Publish government transparency reports** that disclose the volume, nature, and legal basis for requests made to companies to share user information or restrict speech. This should be a fundamental component of any nation's commitment to open government.[66]

- **Ensure that laws and regulations allow companies to be transparent and accountable** with users about how they receive and handle government requests.

- **Carry out human rights due diligence to ensure that laws and regulations governing ICT sector companies do not have a negative impact on internet users' freedom of expression and privacy** as defined by the Universal Declaration of Human Rights[67] and international human rights instruments such as the International Covenant on Civil and Political Rights.[68]

- **Reform surveillance-related laws** and practices to comply with the thirteen "Necessary and Proportionate" principles,[69] a framework for assessing whether current or proposed surveillance laws and practices are compatible with international human rights norms.

- **Require companies to implement effective mechanisms for grievance and remedy** that are accessible to users who believe that their freedom of expression and privacy rights have been violated in connection with the use of companies' products and services.

- **Limit legal liability imposed on companies for their users' speech and other activities,** consistent with the Manila Principles on Intermediary Liability, a framework of baseline practices and standards to ensure that regulation of ICT sector companies does not result in the violation of users' rights.[70]

- **Respect the right to anonymous online activity** as central to freedom of expression, privacy and human rights. Refrain from requiring companies to document users' identities when it is not essential to provision of service.

- **Develop effective data protection regimes and privacy regulations** in consultation with industry and civil society, with impact assessments to ensure that the laws can avoid unintended consequences for freedom of expression.

- **Require companies to clearly disclose to users the full lifecycle of their information,** from collection to use to sharing to retention and deletion.

- **Require companies to give users more control over the collection and sharing of their information,** and to clearly disclose how users can exercise such control.

- **Do not enact laws and policies that undermine encryption.** Strong encryption is vital not only for human rights but also for economic and political security.[71]

- **Support appropriate incentives for companies to adopt industry standard security practices** and encourage appropriate disclosure to users.

- **Encourage companies to implement and disclose appropriate policies and procedures for data breaches**, including through relevant legislation.

COMPANY REPORT CARDS

APPLE INC.

● **Internet and mobile**

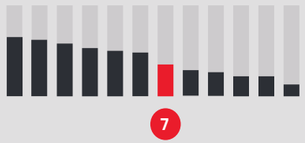
Key Findings:

- Despite its strong public defense of users' privacy, Apple disclosed no clear commitments or policies demonstrating respect for users' freedom of expression.
- Apple disclosed how it handles and complies with government requests to hand over user information, but published no data about government or private requests it receives to restrict content or to remove apps from its app store.
- Apple led most of its peers for disclosure of its encryption policies but could do more to explain its security policies including those for responding to data breaches.

OVERALL SCORE

35%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **iMessage** (Messaging & VoIP)
- **iCloud** (Cloud storage)
- **iOS** (Mobile ecosystem)

ANALYSIS

Apple placed seventh out of the 12 internet and mobile companies and ninth in the overall Index, scoring lower than any other U.S.-based company evaluated. This was the first year Apple was evaluated. Despite Apple's high-profile stance in defense of users' privacy, the company disclosed few commitments or policies that would indicate respect for users' freedom of expression.[1] For instance, the company provided little information about how it handles government or private requests to restrict content, and provided no data about government requests to remove apps from its app store. Apple also lacked disclosure of governance and accountability mechanisms around the implementation of its commitments and policies related to privacy or freedom of expression. Although considered an industry leader in user privacy and security, Apple's commitments in this regard were not always clearly reflected in its privacy-related policies across all of its services evaluated, particularly with Apple's iOS mobile ecosystem.[2]

About Apple Inc.

Apple Inc. designs, manufactures, and sells a range of computers, smartphones, media players, and other devices. The company also produces operating system software (Mac OS for computers and iOS for mobile) and application software. Other services include iMessage, a messaging application that works across Apple devices and iCloud, a cloud storage service. Apple sells and delivers applications through its App Store.

Market Cap: USD 693,173 million[3]
NASDAQGS: AAPL
Domicile: United States
Website: www.apple.com

[1] Robert Hackett, "Here's How Apple Balances Data Analysis with Privacy," Fortune, June 13, 2016, http://fortune.com/2016/06/13/apple-wwdc-event-privacy/; Andy Greenberg, "Apple's Latest Selling Point: How Little It Knows About You," Wired, June 8, 2015, https://www.wired.com/2015/06/apples-latest-selling-point-little-knows/.
[2] For our evaluation of mobile ecosystems, see: https://rankingdigitalrights.org/index2017/findings/mobileecosystems.
[3] S&P Capital IQ, accessed February 13, 2017.

GOVERNANCE 17%

Apple ranked 14th out of the 22 companies in the Governance category, with the lowest score on this set of indicators of any U.S.-based company. While the company published a commitment to respect users' privacy, it made no similar commitment to respect users' freedom of expression (G1). It disclosed senior-level oversight over privacy issues but made no reference to similar oversight over freedom of expression issues within the company (G2). It disclosed no information about whether it conducts any form of human rights due diligence (G4) or evidence of engaging with stakeholders to address freedom of expression and privacy concerns (G5). The company also offered little evidence of a substantive grievance and remedy mechanism enabling users to issue complaints against the company for infringement of their freedom of expression or privacy (G6).

FREEDOM OF EXPRESSION 22%

Apple ranked eighth among the 12 internet and mobile companies in the Freedom of Expression category, scoring slightly better than Mail.Ru and Samsung.

Content and account restriction requests: Apple provides less information on these indicators than most other internet and mobile companies, performing better only than Tencent, Baidu, Samsung, and Mail.Ru (F5-F7). Apple's transparency report included data on requests it received to restrict users' accounts but it disclosed very little information about its process for responding to requests to restrict content on its platforms, or data about these requests (F5, F6). Apple should disclose its processes for responding to requests it receives from governments to restrict apps in its app store, as well as the volume and nature of these requests, as these requests are becoming an increasingly prominent threat to freedom of expression around the world.[4]

Identity poilcy: Apple disclosed it might require users in certain jurisdictions to verify their identity with a government-issued identification, in compliance with local law (F11).[5]

PRIVACY 48%

Apple placed seventh out of the 12 internet and mobile companies evaluated, scoring lower than all U.S. companies in this category.

Handling of user information: Similar to other companies, Apple fell short of clearly explaining to users how it handles their information (P3-P9). The company 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). Apple provided even less information regarding if and how users can obtain all the information the company holds on them (P8). However the company received the highest score of any company in the Index for clearly disclosing it does not collect user information from third-party websites through technical means (P9).

Requests for user information: Apple lagged behind most of its U.S. peers in its disclosure of government and private requests for user information (P10, P11), although no company received full credit on these indicators. Like most companies, Apple disclosed its process for responding to government requests but provided no information about whether or how it has handled requests from private parties (P10). In its transparency report it disclosed data on the number of government requests it received, broken out by country, but it did not list the number of requests received for real-time user data (only for stored content) (P11). If it does not respond to real-time access requests because user communications are end-to-end encrypted, Apple should state this.

Security: Apple disclosed less than Google, Yandex, and Microsoft about its security policies, despite consensus in the technical community that its products are among the most secure on the market.[6] Apple did not fully disclose its internal security oversight processes, including whether it commissions external audits on products and services (P13). Like most companies, Apple offered no information about its process for responding to data breaches (P15). Apple's disclosure regarding its encryption policies was notably better than most other companies evaluated (P16), disclosing that it encrypts users' communications by default. For iMessage and the Apple mobile ecosystem, it disclosed that end-to-end encryption is enabled by default.

[4] "Clearing Out the App Stores: Government Censorship Made Easy," *New York Times*, 18 January 2017, https://www.nytimes.com/2017/01/18/technology/clearing-out-the-app-stores-government-censorship-made-easier.html?_r=0.
[5] "Privacy Policy," Apple, accessed February 17, 2017, http://www.apple.com/privacy/privacy-policy/.
[6] The state of mobile device security: Android vs. iOS, http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/.

BAIDU, INC.

● Internet and Mobile

Key Findings:

- Baidu does not publicly commit to respect human rights, and has weak disclosure of policies affecting users' freedom of expression and privacy.
- China's challenging legal environment does not excuse the extent of Baidu's poor disclosure about the collection and other handling of user information, or lack of basic information about its security practices.
- While Chinese law makes it unrealistic to expect companies to disclose most information about government requests, the company should make clearer disclosures about whether and how it shares data with non-governmental parties and under what circumstances.

OVERALL SCORE

13%

INTERNET AND MOBILE RANK

SERVICES EVALUATED

- **Baidu Search** (Search engine)
- **Baidu Cloud** (Cloud storage)
- **Baidu PostBar** (Social networking & blog)

ANALYSIS

Baidu was the lowest-ranked internet and mobile company evaluated and received the third-lowest score in the Index overall. Baidu is new to the Index, joining Tencent as the second Chinese company evaluated. The 2016 *Freedom on the Net* report by Freedom House rated China's internet environment as "Not Free," with China scoring the lowest of all countries reviewed.[1] While many aspects of Baidu's poor performance can be blamed on China's legal and regulatory environment, the company can be held responsible for poor disclosure on most of the indicators related to how a company handles and secures user information. The fact that Tencent outperformed Baidu on several such indicators (in some cases substantially) proves that the legal environment does not fully excuse Baidu's poor performance.[2]

About Baidu, Inc.

Baidu Inc. provides internet search services, in China and internationally. Other services offered include cloud storage, maps, an encyclopedia, among others. Baidu PostBar is an online social network based on discussion topics that are closely integrated with Baidu Search. Baidu also provides online marketing services, from which it derives the majority of its revenue.[3]

Market Cap: USD 63,939 million[4]
NasdaqGS: BIDU
Domicile: China
Website: www.baidu.com

[1] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/china**.
[2] For our comparative analysis of Baidu and Tencent, see: **https://rankingdigitalrights.org/index2017/findings/china**.
[3] "Company Overview," Baidu, accessed February 22, 2017, **http://ir.baidu.com/phoenix.zhtml?c=188488&p=irol-homeprofile**.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 0%

Baidu was the only company in the entire Index to receive no credit in the Governance category. The company did not publicly commit to uphold freedom of expression or privacy as human rights (G1), or give any evidence of senior-level oversight over these issues (G2). It did not disclose an employee training or whistleblower program related to freedom of expression and privacy (G3), if it conducts human rights due diligence (G4), or if the company engages with stakeholders on freedom of expression or privacy issues (G5). Baidu also offered no evidence of grievance and remedy mechanisms for users to report infringements of their freedom of expression and privacy (G6).

FREEDOM OF EXPRESSION 13%

Baidu scored lowest of all internet and mobile companies in the Freedom of Expression category, just below Tencent.

Content and account restrictions: Baidu disclosed less on these indicators than any internet and mobile companies evaluated (F3, F4, F8). The company received some credit for its disclosure of what types of content or activities are prohibited on its services (F3). Notably, this indicator rewards companies for the clarity of their rules, rather than for respecting users' freedom of expression rights *per se*. Baidu did not disclose whether it notifies users when their content or accounts have been restricted (F8).

Content and account restriction requests: Baidu was one of only two internet and mobile companies to receive no credit on these indicators (F5-F7). It disclosed no information about its process for responding to government or private requests to restrict content or accounts (F5), nor did it publish data about these requests it receives (F6, F7).

Identity policy: The company disclosed that it requires users to verify their identity with a government-issued ID for all services. A rule issued by the standing committee of the National People's Congress in 2012 requires internet companies to do so (F11).[5]

PRIVACY 17%

Baidu had greater disclosure in the Privacy category, although it scored substantially lower than all other internet and mobile companies evaluated, including Tencent.

Handling of user information: Baidu disclosed less than all internet and mobile companies about how it handles user information (P3-P9). It provided some disclosure of the types of user information it may collect (P3), but gave less information about what is shared (P4), and why (P5). Baidu disclosed nothing about how long it retains this information (P6). The law requires retention for 60 days but does not forbid disclosure of that fact.

Requests for user information: Baidu disclosed almost nothing about how it handles government and private requests for user information, earning equally low scores on these indicators as Tencent (P10-P12). While Chinese law makes it unrealistic to expect companies to disclose most information about government requests, Baidu should be able to reveal if and when it shares data with private parties and under what circumstances. The company did not disclose if it notifies users when governments or private parties request their information (P12). Notably, the Baidu PostBar user agreement states that the service only complies with government requests for user information, or with requests for user information that the user has made public, but it is unclear if this policy also pertains to other Baidu services.

Security: Baidu had the least amount of disclosure of all internet and mobile companies on this set of indicators (P13-P18). Baidu disclosed no institutional processes to ensure the security of its products and services (P13) or address data breaches (P15). Unlike Tencent it disclosed no information about efforts to address security vulnerabilities (P14).

[5] "National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection," China Copyright and Media, December 27, 2012, **https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/**.

FACEBOOK, INC.

● Internet and Mobile

Key Findings:

- Facebook trailed behind the top performers in the Index with less overall disclosure of policies affecting users' freedom of expression and privacy.
- At the corporate level, Facebook improved its disclosure of how it implements commitments to freedom of expression and privacy since the company was evaluated by this Index in 2015.
- Facebook should publish data about content and accounts it removes for violations of its rules, improve its transparency reporting on content removals, and improve disclosures about how it handles user information.

OVERALL SCORE

53%

INTERNET AND MOBILE RANK

4

SERVICES EVALUATED

- **Facebook** (Social networking)
- **Instagram** (Video & photo sharing)
- **Messenger** (Messaging & VoIP)
- **WhatsApp** (Messaging & VoIP)

ANALYSIS

Facebook placed fourth out of 12 internet and mobile companies evaluated and fourth in the Index overall.[1] Since it was first evaluated in the 2015 Index, Facebook clarified some of its Instagram and WhatsApp policies, thereby improving its scores. Specifically, Facebook's most recent transparency report—which covered requests for content removal and requests for user data—clearly stated that the information applies to Facebook, Messenger, WhatsApp, and Instagram.[2]

Despite some notable improvements, there are several areas where Facebook's policy disclosure could be improved. Transparency about requests it receives to remove content or deactivate accounts was less comprehensive than its data on government requests for user information. Like many companies in the Index, Facebook did not disclose any data about the volume and nature of content it removes or accounts it restricts due to the enforcement of its own terms of service, nor did it disclose information about its policies for responding to possible data breaches.

About Facebook, Inc.

Facebook, Inc. operates social networking platforms for users globally. Lead among these are: the Facebook mobile app and website; Messenger, a mobile-to-mobile messaging application; Instagram, a mobile photo and video sharing app; and WhatsApp Messenger, a cross-platform mobile messaging application.

Market Cap: USD 387,807 million[3]
NasdaqGS: FB
Domicile: United States
Website: www.facebook.com

[1] For Facebook's performance in the 2015 Index, see: https://rankingdigitalrights.org/index2015/companies/facebook.
[2] "About the Reports," Facebook, accessed February 18, 2017, https://govtrequests.facebook.com/about/.
[3] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 81%

Facebook tied with Vodafone for the second-highest score of all 22 companies evaluated in the Governance category, behind Microsoft and Yahoo. Facebook's performance on governance indicators improved substantially since the 2015 edition of the Index. Facebook became a member of the Global Network Initiative (GNI) in 2013, and in 2016 the GNI completed its first independent assessment of the company, finding Facebook in compliance with GNI principles for how companies handle government demands affecting freedom of expression and privacy.[4] Facebook provided evidence that the company's senior leadership exercises oversight of issues related to freedom of expression and privacy, an improvement from 2015 (G2). Facebook's disclosure related to its human rights due diligence also improved, as the company committed to conduct regular human rights impact assessments (G4).

FREEDOM OF EXPRESSION 41%

Facebook ranked sixth out of 12 internet and mobile companies in the Freedom of Expression category, below almost all other U.S. companies.

Content and account restrictions: Facebook disclosed less than Kakao and Google about what types of content and activities are prohibited on its services, but more than all other internet and mobile companies evaluated (F3). However, it provided no data about the actions it takes to enforce its terms of service rules (F4). As with most companies, Facebook disclosed nothing about whether it grants government authorities or private parties priority consideration when flagging content for terms of service violations.

Requests for account and content restrictions: Facebook scored in the top half of internet and mobile companies on this set of indicators, though it offered less disclosure than Google, Yahoo, and Kakao (F5-F7). It offered some disclosure of its process for responding to government and private requests for content and account restrictions (F5). Its disclosure of data about the government requests it receives was less comprehensive (F6). It also provided little information about requests it receives from private parties to remove content or restrict accounts (F7).

Identity policy: WhatsApp and Instagram disclosed that users can register an account without verifying their identity with a government-issued ID. Facebook's social network and Messenger app, however, disclosed they may require users to do so (F11).[5]

PRIVACY 49%

Facebook received the fifth-highest score out of 12 internet and mobile companies in the Privacy category,

Handling of user information: Facebook fell short of explaining how it handles user information, placing behind Twitter, Google, Microsoft, Yahoo, and Kakao on these indicators (P3-P9). While the company offered some disclosure about what types of user information it collects (P3), it revealed less about what it shares and with whom (P4), for what purpose (P5), and for how long it retains it (P6). Its diclosure of options users have to control what information the company collects, retains, and uses was especially poor (P7).

Requests for user information: Facebook disclosed less than Microsoft, Twitter, and Google about how it processes and complies with government requests for user information (P10, P11). However, it received the second-highest score of internet and mobile companies, after Twitter, for its disclosure of data about requests for user information it receives from governments and other third parties (P11).

Security: Facebook disclosed less than many of its peers but more than Twitter about its security policies (P13-P18). It revealed little about its internal security oversight over its products and services (P13) or about user account security features and practices (P17). Facebook received higher than average marks for dislcosure of its encryption policies (P16). For the Facebook social network, Facebook Messenger, and WhatsApp, the company clearly stated that the transmission of user communications is encrypted by default, and that it encrypts these transmissions using unique keys.

[4] "Public Report on the 2015/2016 Independent Company Assessments," Global Network Initiative, July 2016, http://globalnetworkinitiative.org/sites/default/files/Public-Report-2015-16-Independent-Company-Assessments.pdf.
[5] "Help Center - What Types of ID Does Facebook Accept?" Facebook, https://www.facebook.com/help/159096464162185?helpref=faq_content.

GOOGLE INC.

● Internet and Mobile

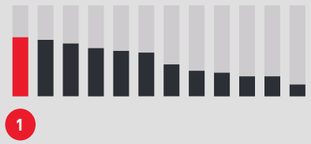
Key Findings:

- Google was the top-ranked company of the 2017 Index, due to its strong disclosure of policies affecting freedom of expression and privacy relative to its peers.
- Google disclosed less evidence that it has implemented its commitments to freedom of expression and privacy at the corporate level than in 2015, and in comparison to several of its U.S. peers.
- While earning top marks for disclosure of privacy-related policies, Google could improve its disclosure of what user information it collects, shares, and retains.

OVERALL SCORE

65%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Google Search** (Search engine)
- **Gmail** (Email)
- **YouTube** (Video sharing)
- **Android** (Mobile ecosystem)

ANALYSIS

Google ranked first in the 2017 Index.[1] A founding member of the Global Network Initiative (GNI), Google outperformed all internet and mobile companies and received the highest score overall. For the first time, this year's evaluation included Google's Android mobile ecosystem, which outperformed Apple's iOS and Samsung's implementation of Android.[2] But there is much room for improvement. While Google bested all other companies in the Freedom of Expression and Privacy categories, it fell noticeably short in the Governance category, especially next to other GNI member companies. In addition, Google could significantly improve public disclosures about policies affecting its Android mobile ecosystem. Poor disclosure on the Android mobile ecosystem, relative to the other Google services evaluated, pulled down the company's overall score. In addition, while Google performed well across most privacy indicators, the company could improve its disclosure related to how it collects, shares, and retains user information.

About Google Inc.

Google Inc. [a subsidiary of Alphabet Inc. since October 2015[3]] is a global technology company that develops a range of products and services that facilitate discovery and management of information. Alongside its significant suite of consumer applications and devices, Google also provides advertising services, consumer hardware products, and systems software, like its open-source mobile operating system, Android.

Market Cap: USD 569,884 million (Alphabet Inc.)[4]
NASDAQGS: GOOGL
Domicile: United States
Website: www.google.com

[1] For Google's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/google**.
[2] For our evaluation of mobile ecosystems, see: **https://rankingdigitalrights.org/index2017/findings/mobileecosystems**.
[3] "G Is for Google," Alphabet, accessed February 22, 2017, **https://abc.xyz/**.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 71%

Google ranked sixth out of the 22 companies evaluated in the Governance category. While Google articulated a clear commitment to upholding users' freedom of expression and privacy rights (G1),[5] it did not disclose evidence of board-level or even executive-level oversight over these issues within the company (G2). This marked a decline in clarity of disclosure about governance and accountability mechanisms across Google's global operations since the company's corporate restructuring under Alphabet. In addition, although Google committed to conduct human rights risks assessments when entering new markets, we found no evidence that it conducts assessments of risks associated with the processes and mechanisms used to enforce its terms of service (G4). It also had notably weak remedy and grievance mechanisms enabling users to submit complaints about infringements to their freedom of expression or privacy (G6).

FREEDOM OF EXPRESSION 60%

Google was the top-performing internet and mobile company in the Freedom of Expression category.

Content and account restrictions: Google disclosed less than Twitter, Kakao, and Microsoft but more than the rest of its peers on these indicators (F3, F4, F8). It provided detailed information about what types of content and activities are prohibited, including some information about its internal processes for identifying content and activities that violate the company's terms of service (F3). Google was one of only three companies evaluated to disclose any information about content or accounts it restricts for terms of service violations (F4). In 2015, Google reported removing 92 million videos from YouTube for terms of services violations, but there has been no follow-up disclosure since and evidence of similar disclosures for other Google services evaluated.[6]

Content and account restriction requests: Google disclosed more than any other company in the Index about how it handles government and private requests to restrict content and accounts (F5-F7). Its transparency report included detailed data about government requests to restrict content or accounts (F6). Notably, Google's transparency report includes data on government requests to remove apps from Google Play. Google's disclosure of private requests was significantly less detailed than that of Kakao, Twitter, Microsoft, and Yahoo (F7).

Identity poilcy: Google lost points on F11, which evaluates whether companies require users to verify their identity in order to use its services. While for Gmail, YouTube and Google Play, users are not required to confirm their identity, app developers are required to do so (by making a small commercial transaction).

PRIVACY 65%

Google earned the highest score among internet and mobile companies in the Privacy category.

Handling of user information: Google performed poorly on a number of indicators related to disclosure of how it handles user information. The company provided some information about the user information it collects (P3), but was less transparent about what it shares and for how long it retains it (P4, P6). Laudably, Google disclosed more than any other company about options users have to obtain the information the company holds about them (P8).

Requests for user information: Google disclosed less than Microsoft and on par with Twitter about how it handles government and private requests for user information (P10, P11). It demonstrated a clear commitment to complying with government and private requests for user information only when prescribed by law, as well as to challenging overbroad requests.

Security: Google tied with Kakao and received full credit for disclosing internal security measures that limit access to user data (P13), and received the second-highest score for clear policies addressing security vulnerabilities, including having a bug bounty program (P14). Similar to most companies evaluated, Google disclosed nothing about how the company notifies users and other affected parties about data breaches and steps taken to mitigate damage (P15). But it earned the top score for clearly disclosing its encryption policies for each service, ahead of the second-best scoring companies on this indicator, Apple and Yandex (P16).

[5] "Google Code of Conduct," Alphabet Investor Relations, April 11, 2012, **https://abc.xyz/**.
[6] "Why Flagging Matters," Official YouTube Blog, September 15, 2016, **https://youtube.googleblog.com/2016/09/why-flagging-matters.html**.

KAKAO CORP.

● Internet and Mobile

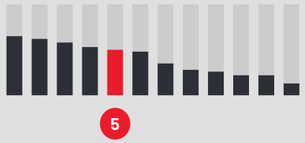
Key Findings:

- Kakao had strong disclosure of policies affecting freedom of expression and led its peers in disclosing how it handles user information.
- Kakao can improve its governance and due diligence policies to ensure that its business operations at all levels maximize respect for freedom of expression and privacy.
- South Korean regulations such as those related to data protection, terms of service, and remedy bolstered Kakao's performance on specific indicators.

OVERALL SCORE

50%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Daum Search Engine** (Search engine)
- **Daum Mail** (Email)
- **Kakao Talk** (Messaging & VoIP)

ANALYSIS

Kakao ranked fifth out of the 12 internet and mobile companies evaluated and received the fifth-highest score in the Index overall.[1] While South Korea is rated "partly free" by Freedom House's 2016 *Freedom on the Net* report, Kakao performed better in the Index than some companies headquartered in the U.S.[2] It ranked solidly ahead of Twitter and Apple, with nearly double the overall score of Samsung, the other South Korean company evaluated for the 2017 Index.

Notably, South Korean regulatory requirements helped to boost the company's performance in a number of areas. For example, South Korean law requires grievance mechanisms. Kakao's clear terms of service and privacy policies, and commitment to notify users about changes, can also be credited to legal and regulatory factors. However, South Korean law prevents disclosure in other areas. Legal requirements around the removal of copyrighted and defamatory content make it difficult to disclose information about certain types of lawful requests to remove or restrict content. The law also inhibits user notification about certain types of government requests for user information. Kakao would benefit from clearer explanation to users about how the law affects what it does not disclose.

About Kakao Corp.

Kakao Corp. delivers mobile platforms to consumers in South Korea. The company's services cover web-based mail and messaging, search services, maps and location services, as well as media, content, and gaming platforms. Further segments include web services, advertising solutions, software, and development and publishing services.

Market Cap: USD 4,945 million[3]
KOSDAQ: A035720
Domicile: South Korea
Website: www.kakao.com

[1] For Kakao's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/kakao**.
[2] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/south-korea**.
[3] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 35%

Kakao ranked ninth in the Governance category, topping Samsung and Twitter, due mainly to above-average perfomance on two indicators. It disclosed some engagement with stakeholders (G5), and its disclosure on grievance and remedy (G6) was greater than that of any other internet and mobile company evaluated. While this disclosure was largely due to requirements under South Korean law,

Kakao went beyond the law by providing users with an appeals mechanism when content is removed in response to defamation claims. On other governance indicators, there are no regulatory obstacles to further strengthening and clearly disclosing accountability and due diligence processes across the board (G1-G4).

FREEDOM OF EXPRESSION 55%

Kakao was the second-best performer in the Freedom of Expression category, behind Google.

Terms of service: Kakao clearly disclosed and documented changes to its terms of service (F2), and disclosed more about how it enforces its terms than any other company in the Index (F3). However, it published no data about content removed or accounts deactivated when enforcing its terms (F4).

Content and account restriction requests: Next to its peers, Kakao had strong disclosure about government and private requests to remove content or restrict accounts (F5-F7).

Disclosure about its process for responding to government and private requests (F5) was above average, although disclosure about government requests was weaker than about private requests. Published data about government requests to restrict content or accounts (F6) contained no information about requests from outside of Korea. Notably, however, Kakao's transparency reporting about private requests (F7) disclosed more types of data with more granularity than any other company in the Index. Kakao also earned the highest score (albeit fewer than half the possible points) for notifying users when content is removed or an account is deactivated (F8).

PRIVACY 53%

Kakao received the fourth-highest score of the 12 internet and mobile companies evaluated, tying with Twitter, in the Privacy category.

Handling of user information: Kakao received the highest score in the Index for disclosure about collection and sharing of user information, although the clarity of its policies was stronger for Kakao Talk (chat service) than for its search or mail services (P3, P4). Disclosure about the purpose for collecting and sharing user information was less detailed (P5). Kakao earned the second-highest score after Twitter for disclosure about how long data is retained (P6). Disclosures about the extent to which users can control the collection, use, and retention of their information (P7), and options users have to obtain all of the information the company holds about them was around average (P8). It disclosed nothing about whether it collects user information from third parties (P9), although it is required by law to make disclosures if it engages in such a practice.

Requests for user information: Kakao disclosed less about how it handles government and private requests for user information than most U.S. internet and mobile companies evaluated, but more than the rest of its peers (P10, P11). However, the law did inhibit some of the company's disclosure about user notification for certain types of government requests: Under the Protection of Communications Secrets Act, the authority requesting the user's information is responsible for any notification, and all other parties involved must keep all information about the process confidential.[7]

Security and encryption: Kakao ranked in the top half of internet and mobile companies on this set of indicators, though it offered less disclosure than Google, Yandex, Microsoft, and Apple (P13-P18). Kakao received a perfect score along with Google for institutional oversight and due diligence on data security (P13). It provided no information about measures taken to address vulnerabilities (P14) or disclosures about data breaches (P15).

[4] "Act on Promotion of Information and Communications Network Utilization and Information Protection (ICNA)," (1986).
[5] "Act on the Regulation of Terms and Conditions," (1986).
[6] "Copyright Act," (1957), and "Act on Promotion of Information and Communications Network Utilization and Information Protection," (1986).
[7] "Protection of Communications Secrets Act" (1993).

MAIL.RU GROUP LIMITED

● **Internet and Mobile**

Key Findings:

- Mail.Ru failed to clearly disclose policies affecting users' freedom of expression and privacy.
- The company disclosed nothing about how it handles government and private requests to restrict content and accounts, or to hand over user information. Russian authorities may have direct access to user information without needing to request it, but Mail.Ru could disclose its process for handling private requests.
- Mail.Ru ranked lower than Yandex, the other Russian internet company evaluated, which disclosed more about its security practices and how it handles user information. These differences highlight areas in which Mail.Ru could improve.

OVERALL SCORE

22%

INTERNET AND MOBILE RANK

SERVICES EVALUATED

- **Mail.Ru** (Email)
- **Mail.Ru Agent** (Messaging & VoIP)
- **Vkontakte** (Social networking & blog)

ANALYSIS

Mail.Ru ranked 10th of 12 internet and mobile companies evaluated and 14th in the Index overall.[1] As a Russian company, Mail.Ru faces clear challenges: The 2016 *Freedom on the Net* report by Freedom House rated Russia's internet environment as "Not Free."[2] According to Freedom House, Russian companies must comply with laws that grant authorities broad powers to create internet "blacklists," and participate in a mass surveillance program, SORM, which allows authorities to intercept communications and metadata. But these constraints do not fully explain the company's weak disclosure in a number of other areas. Mail.Ru scored six percentage points lower than Yandex, the other Russian internet company evaluated, highlighting areas where immediate improvement is possible. For Mail.Ru this includes disclosure of its processes for handling government and private requests for content and account restrictions, and requests to hand over user information, indicators on which Yandex scored higher.[3]

About Mail.Ru

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

Market Cap: USD 3,751 million[4]
LSE: MAIL
Domicile: Russia
Website: www.corp.mail.ru

[1] For Mail.Ru's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/mailru/**.
[2] "Freedom on the Net," (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/russia**.
[3] For our comparative analysis of Mail.Ru and Yandex, see: **https://rankingdigitalrights.org/index2017/findings/russia**.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 7%

Mail.Ru scored poorly in the Governance category, earning the fourth-lowest score of all 22 companies evaluated, ahead of Axiata, Ooredoo, and Baidu. It received a small amount of credit on just two of the six indicators in this category. It disclosed a whistleblower program, although not specifically for reporting freedom of expression and privacy concerns (G3). It also disclosed an avenue for users to file complaints, including about blocked accounts, but offered no options for users to file privacy-related grievances (G6).

FREEDOM OF EXPRESSION 21%

Mail.Ru received the fourth-lowest score of the 12 internet and mobile companies evaluated in this category, placing just ahead of Samsung, Tencent, and Baidu.

Content and account restrictions: Mail.Ru disclosed far less than most other internet and mobile companies on these indicators (F3, F4, F8). While the company received some credit for disclosing what types of content and accounts are prohibited on its services, it also disclosed it can delete user content without notice and without explanation (F3). Mail.Ru did not provide data about the content or accounts it restricts for violating its terms (F4), nor did it disclose a policy to notify users when it restricts content or their account (F8).

Content and account restriction requests: Mail.Ru disclosed far less than most other internet and mobile companies, with the exception of Samsung, Baidu, and Tencent, on these indicators (F5-F7). Although there are no laws prohibiting Russian companies from disclosing information about government requests to restrict or block content or accounts, the company provided only minimal information about its processes for responding to these types of requests (F5) and no data about the number of requests from governments or private parties it receives or complies with (F6, F7).

Identity policy: Mail.ru's VKontakte, the social networking service, disclosed that it requires users to provide a mobile phone number and may ask to verify a user's real identity in case a user needs tech support.[5] Russian internet service providers and telecommunications companies are legally required to verify the identities of their users, but this requirement does not apply to companies such as Mail.Ru.

PRIVACY 26%

In the Privacy category, Mail.Ru had the second-lowest score of 12 internet and mobile companies, scoring better than only Baidu.

Handling of user information: Mail.Ru scored lower than all other internet and mobile companies except Baidu on these indicators (P3-P9). The company disclosed more information about what types of user information it collects (P3), than about what information it shares (P4), for what purpose (P5), and for how long it retains it (P6). Russian law does not prevent companies from fully disclosing user information retention policies.

Requests for user information: Mail.Ru and Samsung were the only two internet and mobile companies that did not disclose any information on policies for responding to requests by governments and private parties for user information (P10-P11). The company also provided no information about whether it notifies users when information has been requested about them (P12). However, since Russian authorities may have direct access to communications data through SORM, Russian companies may not be aware of the number of times, or for which users, government authorities access user information.

Security: Mail.Ru disclosed little about its security policies, but more than four other internet and mobile companies, including Twitter (P13-P18). Like most companies, it offered no information about its process for responding to data breaches (P15). While it disclosed that the transmissions of users' communications are encrypted by default, the company disclosed little else about its encryption policies, particularly in comparison to Yandex, the other Russian internet company evaluated (P16).

[5] "VK Privacy Policy," VK, accessed February 17, 2017, **https://vk.com/privacy**.

MICROSOFT CORP.

● **Internet and Mobile**

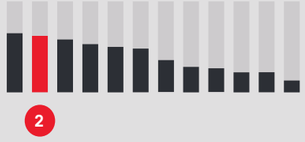
Key Findings:

- One of the top performers in the Index, Microsoft disclosed strong implemenation of its commitment to human rights and to users' freedom of expression and privacy.
- New transparency reporting improved Microsoft's disclosure of policies affecting freedom of expression, including how the company handles government and private requests to restrict content or accounts.
- Microsoft disclosed more than all of its peers about its process for handling government and private requests for user information, but could better explain what user information it collects, shares, and retains.

OVERALL SCORE

62%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Bing** (Search engine)
- **Outlook.com** (Email)
- **Skype** (Messaging & VoIP)

ANALYSIS

Microsoft was the second-ranked internet and mobile company evaluated and received the second-highest score in the Index overall, just after top-ranked Google.[1] A founding member of the Global Network Initiative (GNI), Microsoft disclosed a strong commitment to freedom of expression and privacy. It made a number of improvements since the 2015 Index: Microsoft's new Transparency Hub, launched in late 2015, resulted in increased scores across a number of freedom of expression indicators.[2] In January 2017 Microsoft issued a human rights report with detailed information about the actions the company took in 2016 to implement its human rights commitments, which boosted its performance in the Governance category.[3]

Despite its strong performance, there are areas for improvement. Microsoft could be more transparent about its process for enforcing its terms of service and do more to clarify how it handles user information.

About Microsoft Corp.

Microsoft Corp. develops, licenses, and supports software products, services, and devices worldwide. The company offers a wide range of software and hardware for both consumer and business markets. Major offerings include Windows operating system, Microsoft Office, Windows Phone software and devices, Xbox video game system and related services, Surface devices and accessories, advertising services, server products, Skype, and Office 365 cloud services.

Market Cap: USD 494,562 million[4]
NASDAQGS: MSFT
Domicile: United States
Website: www.microsoft.com

[1] For Microsoft's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/microsoft**.
[2] Corporate Social Responsibility Hub, **https://www.microsoft.com/en-us/about/corporate-responsibility/reports-hub**.
[3] "Microsoft Salient Human Rights Issues Report - FY16" (Microsoft, January 2017), **http://download.microsoft.com/download/0/1/4/014D812D-B2E3-43A0-A89A-16E3C7CD46EE/Microsoft Salient Human Rights Issues Report - FY16.pdf**.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 88%

Microsoft tied with Yahoo for the top score of all 22 companies evaluated in the Index in the Governance category. The company disclosed an explicit commitment to respect freedom of expression and privacy as human rights (G1), evidence of oversight of human rights issues by senior leadership (G2), and employee training and whistleblower programs that addresses these issues (G3). Microsoft's new human rights report included details about the company's human rights impact assessments, with an example of efforts to address freedom of expression risks associated with how it enforces its terms of service (G4). The company could further improve by clearly disclosing that it assesses the freedom of expression and privacy risks associated with its terms of service in a more systematic way, and further clarifying whether it conducts additional evaluation when risk assessments identify concerns.

FREEDOM OF EXPRESSION 53%

Microsoft placed third out of the 12 internet and mobile companies evaluated in the Freedom of Expression category, after Google and Kakao.

Content and account restrictions: Microsoft performed well on this set of indicators compared to other internet and mobile companies, though it offered less disclosure than Twitter and Kakao (F3, F4, F8). It took a step forward by starting to publish data about its terms of service enforcement (F4), specifically related to content it removes for violating its policy on "non-consensual pornography" content on its search engine. It is one of only three companies to receive any credit on the indicator, but could further improve by disclosing data on other types of content it removes for terms of service violations.

Content and account restriction requests: Microsoft placed in the top half of internet and mobile companies on this set of indicators, though it trailed Google, Yahoo, Kakao, and Facebook (F5-F7). Microsoft's Transparency Hub disclosed the company's process for responding to government and private requests to remove content (F5), and some data about requests from government and private parties it receives and complies with (F6, F7). However, the data provided covered only its search engine, Bing.

PRIVACY 59%

Microsoft placed second out of the 12 internet and mobile companies evaluated in the Privacy category, after Google.

Handling of user information:Microsoft disclosed less than Twitter, Google, and Yahoo about how it handles user information, although all companies scored poorly on these indicators (P3-P9). The company did not fully disclose the types of user information it collects, shares or for what purpose (P3, P4, P5). Like most companies, it provided even less information about how long it retains this information (P6). Microsoft tied with Twitter and scored better than all other companies on its disclosure of options users have to control the information it collects, retains, and uses (P7). It also disclosed more than most companies about what options users have to obtain information the company holds about them (P8) and what information is collected about them from third parties (P9).

Requests for user information: Microsoft disclosed more than all of its peers about its process for handling government and private requests for user information (P10), but lagged behind Twitter, Facebook, and Google for disclosure of data on the requests it receives from these third parties (P11). The company earned the second-highest score after Yahoo for disclosing whether it has a policy to notify users about requests for their information (P12).

Security: Microsoft disclosed less than Google and Yandex about its security policies but more than any other internet and mobile company (P13-P18). The company disclosed an internal oversight process to ensure the security of user data (P13), and a bug bounty program to address security vulnerabilities (P14). It scored lower than Facebook, Yahoo, Apple, Yandex, and Google on disclosure of its encryption policies (P16), but along with Yandex was one of two companies to receive full credit for disclosing what measures users can take to secure their own accounts (P17).

SAMSUNG ELECTRONICS CO. LTD.

● **Internet and Mobile**

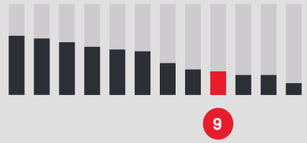
Key Findings:

- Samsung lacked clear disclosure of policies affecting users' freedom of expression and privacy.
- While Samsung made a strong commitment to human rights, it did not disclose whether or how it has institutionalized specific commitments to freedom of expression and privacy at the corporate level.
- Samsung disclosed no information about its handling of government or private requests to remove apps from its app store, or requests for user information. There is no legal obstacle to publishing transparency reports with at least the same level of detail as Kakao, the other Korean company in the Index.

OVERALL SCORE

26%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Samsung's implementation of Android** (Mobile ecosystem)

ANALYSIS

Samsung ranked ninth out of the 12 internet and mobile companies evaluated and placed 13th in the Index overall. Samsung is new to the Index, and its evaluation is based on its Galaxy mobile ecosystem, which along with Apple's iOS and Google's Android rounded out the new mobile ecosystem service category. Of the three mobile ecosystems evaluated, Samsung provided the least amount of disclosure to users about how its policies affect their freedom of expression and privacy.[1]

While South Korea has one of the strongest data protection regimes in the world, Samsung could do more to explain how it adheres to privacy-protecting regulations, as there are no legislative or regulatory barriers preventing Samsung from doing so. The company can clarify its process for policing third-party apps on the Galaxy Apps store, and include such figures in a transparency report that also provides information about government and other third-party requests for user information.

About Samsung Electronics Co. Ltd.

Samsung Electronics Co. Ltd. sells a range of consumer electronics, home appliances, and information technology solutions worldwide. It produces products including televisions, mobile phones, network equipment, and audio and video equipment. Its parent company, Samsung Group, is South Korea's largest public company.[2]

Market Cap: USD 229,830 million[3]
KOSE: A005930
Domicile: South Korea
Website: www.samsung.com

[1] For our evaluation of mobile ecosystems, see: **https://rankingdigitalrights.org/index2017/findings/mobileecosystems**.
[2] "The World's Biggest Public Companies," Forbes, **http://www.forbes.com/global2000/**.
[3] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 22%

Samsung ranked 12th in the Governance category of all 22 companies in the Index, placing behind Twitter but ahead of Apple. The company made a strong public commitment to human rights (G1),[4] but did not disclose senior-level oversight over freedom of expression and privacy issues within the company (G2). It did disclose that it has a unit in charge of employee training on protecting personal information (G3). However, researchers were unable to find meaningful disclosure about human rights due diligence (G4), stakeholder engagement (G5), or grievance and remedy mechanisms (G6).

FREEDOM OF EXPRESSION 20%

Samsung ranked 10th out of the 12 internet and mobile companies on freedom of expression, ahead of only Tencent and Baidu.

Content and account restrictions: For both Galaxy users and app developers, Samsung clearly disclosed what types of content and activities are prohibited (F3), but failed to disclose any information about content or accounts restricted for terms of service violations (F4), nor did it disclose whether it notifies users who attempt to access content that has been restricted (F8).

Content and account restriction requests: Samsung disclosed no information about its process for handling government or private requests to restrict content or user accounts (F5), or about the number of such requests it receives and complies with (F6, F7)

PRIVACY 30%

Samsung received the third-lowest score among internet and mobile companies on privacy, ahead of only Mail.Ru and Baidu.

Handling of user information: Samsung disclosed less than most of the internet and mobile companies about its policies for handling user information. Korean law requires data processors such as Samsung to obtain consent from users when collecting and sharing user information; however, Samsung does not disclose whether users have control over the company's collection, use, or retention of each type of user information it collects (P7). It failed to disclose whether users can obtain a copy of all the information that the company has about them (P8) or whether it collects user information from third parties (P9).

Requests for user information: Samsung disclosed no information about its process for responding to government or private requests for user information (P10), nor did it publish any data about such requests it receives or complies with (P11). It also did not disclose whether it notifies users when their information is requested (P12).

Security: Samsung disclosed little about its security policies compared to its peers (P13-P18). It did disclose a bug bounty program but fell short of committing to refrain from prosecuting security researchers. Samsung disclosed that it receives security updates from Google for its Android operating system but did not specify a timeframe for delivering updates to users (P14). It disclosed nothing about its policy for responding to data breaches (P15) or about the types of encryption that protects user information in storage on its servers, in transit, or at rest on user devices (P16). However, it did disclose ways users can protect their information from unauthorized access to their account (P17).

[4] "Business Conduct Guidelines 2016," (Samsung, 2016), **http://www.samsung.com/us/aboutsamsung/sustainability/sustainabilityreports/download/2016/business-conduct-guidelines-eng-2016.pdf**.

TENCENT HOLDINGS LIMITED

● **Internet and Mobile**

Key Findings:

- Tencent lacked sufficient disclosure of commitments and policies affecting users' freedom of expression and privacy.
- Tencent disclosed more about its policies related to privacy than Baidu, the other Chinese internet company evaluated.
- Chinese law makes it unrealistic to expect companies to disclose most information about government requests, but Tencent could disclose information about its handling of private requests to restrict content or accounts, and private requests for user information.

OVERALL SCORE

22%

INTERNET AND MOBILE RANK

SERVICES EVALUATED

- **Qzone** (Social network)
- **QQ** (Instant messaging)
- **WeChat** (Messaging & VoIP)

ANALYSIS

Tencent ranked 10th out of the 12 internet and mobile companies evaluated and 14th in the Index overall.[1] The 2016 *Freedom on the Net* report by Freedom House rated China's internet environment as "Not Free," with China scoring the lowest of all countries reviewed.[2] While gaps in Tencent's commitments and disclosures can be blamed on China's legal and regulatory environment, there are still areas in which Tencent could improve without regulatory change. Tencent offered different versions of many key documents, including terms of service and privacy policies, for mainland Chinese users and all other users outside of China. Documents offered in English and traditional Chinese characters (used in Hong Kong and Taiwan) contained different substantive content and commitments in some areas, generally with more detail and better disclosure. While all versions were reviewed, only the documents in simplified Chinese (for mainland Chinese users) counted towards the company's Index score.[3]

About Tencent Holdings Limited

Tencent Holdings Limited provides a broad range of internet and mobile value-added services, online advertising services, and ecommerce transactions services to users in China, the United States, Europe, and elsewhere around the world. It is one of the world's largest internet companies.

Market Cap: USD 246,184 million[4]
SEHK: 700
Domicile: China
Website: www.tencent.com

[1] For Tencent's performance in the 2015 Index, see: https://rankingdigitalrights.org/index2015/companies/tencent.
[2] "Freedom on the Net" (Freedom House, November 2016), https://freedomhouse.org/report/freedom-net/2016/china.
[3] For our comparative analysis of Baidu and Tencent, see: https://rankingdigitalrights.org/index2017/findings/china.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 9%

Tencent ranked 17th out of the 22 companies in the Governance category, ahead of Baidu. The company received some credit for committing to protect users' privacy but it made no such commitment to protect users' freedom of expression (G1). To the contrary, its terms of service for mainland Chinese users stated that users' accounts may be terminated for "implicating Tencent in political and public events."[5] The company did provide some information about a general complaints mechanism for users that applied to all services, with WeChat providing somewhat more detail. While Tencent scored below average on this indicator (G6), it nonetheless tied with Google and scored above several companies whose overall Index scores were much higher.

FREEDOM OF EXPRESSION 14%

Tencent ranked 11th of the 12 internet and mobile companies in the Freedom of Expression category, just ahead of Baidu.

Content and account restrictions: Tencent disclosed less than most internet and mobile companies on these indicators (F3, F4, F8), but more than Apple and Baidu. The company offered above-average disclosure of what types of content or activities are prohibited (F3). Notably, this indicator rewards companies for the clarity of their rules, rather than for respecting users' freedom of expression rights *per se*. The company failed to disclose the volume and nature of content or accounts restricted in enforcing these rules (F4), though all companies performed poorly on this indicator. It also failed to disclose a consistent policy to notify users when the company restricts content or accounts (F8).

Content and account restriction requests: Tencent disclosed little about how it handles requests from governments and private parties to restrict content or user accounts, although it scored better on these indicators than Baidu and Samsung (F5-F7). It did not disclose any data about government or private requests for content or account restrictions it receives, or its compliance with these requests (F6, F7).

Identity policy: The company disclosed that it may, depending on applicable laws, require users to verify their identity with a government-issued ID for all services. Network service providers offering internet access or information related services in China are legally required to do so (F11).[6]

PRIVACY 31%

Tencent received the fourth-lowest score among internet and mobile companies evaluated in the Privacy category, ahead of Samsung, Mail.Ru, and Baidu.

Handling of user information: Tencent performed below the internet and mobile company average on this set of indicators (P3-P9). However, it provided strong disclosure of what user information it collects, on par with Facebook, Twitter, Yahoo, and Yandex (P3). But it did not fully disclose the reasons it shares the information it collects (P5), and disclosed nothing about how long it retains user information (P6). The law requires retention for 60 days but does not forbid disclosure of that fact.

Requests for user information: Tencent disclosed almost nothing about how it handles government and private requests for user information, earning equally low scores on these indicators as Baidu (P10-P12). While Chinese law makes it unrealistic to expect companies to disclose most information about government requests, Tencent should be able to reveal if and when it shares user information with private parties and under what circumstances.

Security: Tencent disclosed little about its security policies, scoring better than only Baidu on these indicators (P13-P18). However, the company tied with Twitter, Facebook, and Yandex for the highest score for its disclosure on how it addresses security vulnerabilities (P14).

[5] "Tencent User Service Agreement," QQ.com, accessed February 21, 2017, http://www.qq.com/contract.shtml.
[6] "National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection," China Copyright and Media, December 28, 2012, https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/.

TWITTER, INC.

● Internet and Mobile

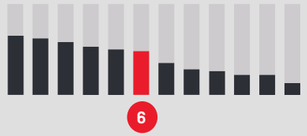
Key Findings:

- Twitter lagged behind most other U.S. companies in disclosing how it has institutionalized its commitments to respect freedom of expression and privacy across its global operations.
- Twitter's flagship social networking service led the field for its disclosure of government and private requests it receives to restrict content and accounts.
- It was unclear if Twitter's policies applied to other services operated by the company, such as Vine and Periscope, bringing down Twitter's overall score.

OVERALL SCORE

48%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Twitter** (Social network)
- **Vine** (Video sharing)
- **Periscope** (Live video streaming)

ANALYSIS

Twitter ranked sixth out of 12 internet and mobile companies and sixth in the Index overall.[1] This year's evaluation included Vine, since the service was included in the 2015 Index and was active during the Index research period, although Vine was discontinued in January 2017. The video streaming mobile app, Periscope, was included for the first time in the 2017 Index. As was the case in 2015, Twitter lacked clear public commitments or disclosed policies for implementing their commitments to respect freedom of expression across its global operations. It was also unclear in many instances if various policies that applied to Twitter's flagship social media service also extended to the Vine and Periscope services. Twitter's overall score in the Index would be substantially higher if the company had disclosed more detailed information on whether or not policies that apply to the flagship Twitter platform also apply to other services.

About Twitter, Inc.

Twitter, Inc. operates as a global social sharing platform. Its products and services allow users to create, share, and find content and short looping and livestreamed videos. Alongside these social services, Twitter provides advertising services and developer tools.

Market Cap: USD 11,052 million[2]
NYSE: TWTR
Domicile: United States
Website: www.twitter.com

[1] For Twitter's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/twitter**.
[2] S&P Capital IQ, Accessed February 13, 2017.
[3] "Twitter for Good | About,"https://about.twitter.com/company/twitter-for-good; "The Twitter Rules," **https://help.twitter.com/articles/18311?lang=en**; "The Tweets Must Flow," **https://blog.twitter.com/2011/the-tweets-must-flow**.

GOVERNANCE 30%

Twitter received the 10th highest score out of the 22 companies in the Index in the Governance category, scoring lower than most U.S. companies. While company blog posts and support pages referenced the company's positions on users' rights to freedom of expression and privacy,[3] these fell short of the type of explicit policy commitment made by many of its peers (G1). Also unlike many of its peers, Twitter offers no publicly accessible evidence of how its policy positions and commitments related to freedom of expression and privacy have been institutionalized through governance and accountability mechanisms across the company. For example, there was no indication of whether Twitter conducts human rights due diligence to identify how aspects of its business may affect freedom of expression and privacy (G4). While Twitter disclosed that it regularly engages with a range of stakeholders on freedom of expression and privacy issues (G5), it is not a member of a multi-stakeholder initiative such as the Global Network Initiative (GNI) whose members not only make commitments but also undergo independent assessment to verify whether they have implemented and institutionalized these principles.

FREEDOM OF EXPRESSION 49%

Twitter ranked fourth out of the 12 internet and mobile companies in the Freedom of Expression category, behind Google, Kakao, and Microsoft.

Content and account restrictions: Twitter provided some disclosure on its process for terms of service enforcement, though it did not indicate if government or private entities receive priority consideration when flagging content for potentially violating the company's rules (F3). Twitter was one of only three companies, including Microsoft and Google, to disclose any data about its terms of service enforcement, reporting the number of accounts it restricted due to terrorist content (F4).[4] But it did not report on other types of content that it removed for violating the company's rules.

Content and account restriction requests: Twitter disclosed less than Google, Yahoo, Kakao, Facebook, and Microsoft about how it handles government and private requests to restrict content or accounts (F5-F7). Its processes for responding to such requests were not clear or consistent across the services evaluated (F5). Twitter provided detailed data about requests it received and complied with, though it did not specify if Periscope and Vine were also included (F6).[5] Twitter's data on requests from private third parties were limited to copyright and trademark violations, though they included Twitter, Vine, and Periscope; Twitter received the second-highest score on this indicator (F7).

Identity policy: Twitter and Microsoft were the only two internet and mobile companies to receive full credit for disclosing that they do not require users to verify their identity with a government-issued ID or other information tied to their offline identity (F11).

PRIVACY 53%

Twitter tied with Kakao for fourth place among internet and mobile companies in the Privacy category, behind Google, Microsoft, and Yahoo.

Handling of user information: Twitter received the highest score of all companies evaluated for this set of indicators (P3-P9). The company clearly disclosed what types of user information it collects (P3) but offered less comprehensive disclosure about what types of user information it shares and with whom (P4). It disclosed more than any other company about how long it retains user information (P6).

Requests for user information: Twitter received the second-highest score on this set of indicators, tying with Google and behind Microsoft (P10-P11). Twitter clearly disclosed its process for responding to government requests for user information but not for private requests (P10). It topped all internet and mobile companies for its transparency reporting on government and private requests it receives to hand over user information (P11).

Security: Twitter provided little information about its security policies, scoring higher only than Baidu and Tencent on these indicators (P13-P18). Like most companies, it failed to disclose any information about how it responds to data breaches (P15). It had one of the lowest scores for its lack of clear disclosure about whether it encrypts user communications and private content (P16).

[4] "Combating Violent Extremism," **https://blog.twitter.com/2016/combating-violent-extremism**.; "An Update on Our Efforts to Combat Violent Extremism," **https://blog.twitter.com/2016/an-update-on-our-efforts-to-combat-violent-extremism**.
[5] "Removal Requests," Twitter Transparency Report, **https://transparency.twitter.com/en/removal-requests.html**.

YAHOO! INC.

● Internet and Mobile

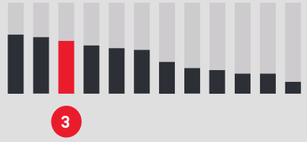
Key Findings:

- Yahoo disclosed a strong commitment to freedom of expression and privacy as human rights at the corporate level and was one of the top-ranked companies in the 2017 Index.
- Yahoo disclosed less about policies affecting users' freedom of expression than users' privacy, including information about the number and types of content or accounts the company restricts for violating its terms of service.
- Yahoo should clarify its policies and procedures for securing user information, including its policies for responding to data breaches.

OVERALL SCORE

58%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Yahoo Mail** (Email)
- **Flickr** (Photo management & sharing)
- **Tumblr** (blogging platform)

ANALYSIS

Yahoo ranked third of the 12 internet and mobile companies evaluated, behind Google and Microsoft, and third in the Index overall.[1] A founding member of the Global Network Initiative (GNI), the company's disclosures related to freedom of expression and privacy are overseen by the Yahoo Business and Human Rights Program, established in 2008 to help integrate human rights-related decision-making into the company's business operations.[2] However, recent revelations about large-scale data breaches at Yahoo highlight why the company's lack of disclosure about its policies for informing affected parties about data breaches and steps taken to mitigate damage should be a concern for users and other stakeholders—though it should be noted that no internet or mobile company evaluated provided disclosures related to data breaches (P15).[3]

About Yahoo! Inc.

Yahoo! Inc. provides a broad range of communication, sharing, and information and content services. Its services include the search platform Yahoo Search, communication and collaboration tools including Yahoo Mail, Yahoo Messenger, and Yahoo Groups, digital content through Yahoo.com, Yahoo Sports, and Yahoo Finance, advertising services, and multiple other services and properties. The Yahoo services evaluated in the Index are all included in an acquisition deal with Verizon Communications, though at the date of this publlication the sale had not closed.

Market Cap: USD 42,964 million[4]
NASDAQGS: YHOO
Domicile: United States
Website: www.yahoo.com

[1] For Yahoo's performance in the 2015 Index, see: https://rankingdigitalrights.org/index2015/companies/yahoo.
[2] Yahoo Business & Human Rights Program, https://yahoobhrp.tumblr.com/post/75544734087/yahoo-business-human-rights-program-yahoo.
[3] "Yahoo Says 1 Billion User Accounts Were Hacked," *The New York Times*, December 14, 2016, https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 88%

Yahoo tied with Microsoft for the highest score of all 22 companies in the Governance category. The company disclosed a clear commitment to freedom of expression and privacy as human rights (G1), evidence of senior leadership oversight of human rights concerns (G2), and provides employee training and a whistleblower program addressing freedom of expression and privacy (G3). As a member of the GNI, Yahoo disclosed that it engages with stakeholders, including civil society, on freedom of expression and privacy issues (G5). Yahoo was the only company to receive full credit for its disclosures about its human rights due diligence processes (G4). As with many companies evaluated in the Index, Yahoo did not disclose sufficient grievance and remedy mechanisms. Its privacy policy indicated how users can contact them with complaints related to privacy concerns, but did not provide further information about its process for receiving and responding to these complaints.

FREEDOM OF EXPRESSION 43%

Yahoo received the fifth-highest score of the 12 internet and mobile companies evaluated in the Freedom of Expression category, behind Google, Kakao, Microsoft, and Twitter.

Content and account restrictions: Yahoo's disclosure of its process for enforcing its terms of service rules (F3) was on par with that of Twitter, though less detailed than that of Google or Kakao. Similar to most (but not all) other companies, Yahoo did not disclose any data about the volume or nature of actions the company takes of its own accord to enforce its rules, such as removing content or restricting users' accounts for violating its terms of service (F4). Given that companies like Microsoft and Twitter are starting to engage in this practice, Yahoo should endeavor to start disclosing this type of data in its next transparency report.

Content and account restriction requests: Yahoo was the second-highest scoring company, behind Google, for this set of indicators (F5-F7). The company received full credit for disclosures on its processes for responding to government requests for account or content restriction, but it provided less thorough disclosure on its processes for content or account restriction requests from private parties (F5).

Identity policy: To set up a Yahoo account (which can be used as a login for Yahoo Mail and Flickr), Yahoo disclosed that it requires that users provide a phone number, which in some jurisdictions can be used (e.g. by law enforcement or other government officials) to connect a user with their offline identity (F11).

PRIVACY 56%

Yahoo received the third-highest score of the 12 internet and mobile companies evaluated in the Privacy category, behind Google and Microsoft.

Handling of user information: Yahoo received the third-highest score of all companies evaluated in the Index for this set of indicators, behind Twitter and Google (P3-P9). Yahoo provided users with greater clarity about what user information it collects and shares (P3, P4) than it did about its reasons for doing so (P5). Yahoo tied with Microsoft for the third-highest score for its disclosures on its policies for retention of user information (P6). Yahoo disclosed more information than most internet and mobile companies about how users can access the information that the company holds about them (P8), with only Google receiving a higher score.

Requests for user information: Yahoo received the second highest score on the indicator related to disclosure of its process for responding to government and other third-party requests for user information (P10), behind only Microsoft. However, it disclosed less than all other U.S. internet and mobile companies about its compliance with government and private requests for user data (P11).

Security: Yahoo disclosed less about its security policies than Google, Yandex, Microsoft, and Apple (P13-P18). Its disclosure of its internal oversight mechanisms to ensure the security of its products was inconsistent across the three Yahoo services evaluated (P13).[5] As noted, Yahoo offered no disclosure of its processes for responding to data breaches (P15) although this was true of all internet and mobile companies in this Index.

[5] "Yahoo Privacy Center," Yahoo, accessed February 21, 2017, https://policies.yahoo.com/us/en/yahoo/privacy/index.htm.

YANDEX N.V.

● Internet and Mobile

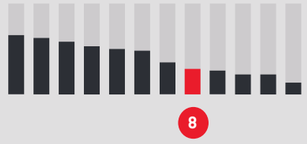
Key Findings:

- While Yandex topped Mail.Ru, the other Russian internet company evaluated, it still failed to sufficiently disclose commitments and policies affecting users' freedom of expression and privacy.
- Yandex disclosed little about how it handles government and private requests for user information. Russian authorities may have direct access to user information without needing to request it, but Yandex could disclose more about its policies and processes for handling requests from non-governmental entities.
- Yandex was among the top-performing companies regarding disclosure of its security policies, but could significantly improve disclosure of how it handles user information.

OVERALL SCORE

28%

INTERNET AND MOBILE RANK



SERVICES EVALUATED

- **Yandex Mail** (Email)
- **Yandex Search** (Search engine)
- **Yandex Disk** (Cloud storage)

ANALYSIS

Yandex ranked eighth out of the 12 internet and mobile companies evaluated, and 12th in the Index overall. The company is new to this year's ranking, joining Mail.Ru as the second Russian internet company evaluated by the Index. Notably, Yandex performed better than Mail.Ru, particularly on privacy-related disclosures, even though both companies operate within the restrictions of the Russian internet environment, which Freedom House rates as "Not Free."[1] Freedom House reports that companies for instance must comply with laws granting authorities broad powers to create internet "blacklists" and to participate in a mass surveillance system, SORM, that allows authorities to access communications and metadata.[2]

About Yandex N.V.

Yandex N.V. provides a range of internet-based services in Russia and internationally. The company's products include the largest search engine in Russia, along with other services including email, cloud storage, and maps.

Market Cap: USD 7,452 million[3]
NASDAQGS: YNDX
Domicile: Russia
Website: www.yandex.com/

[1] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/russia**.
[2] For our comparative analysis of Mail.ru and Yandex, see **https://rankingdigitalrights.org/index2017/findings/russia**.
[3] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 10%

Yandex ranked 16th among all 22 companies evaluated in the Index in the Governance category. However, the company did have some notable disclosures: it disclosed a mechanism for employees and users to report violations to its code of conduct, which includes some aspects of privacy-related issues (G3), and received some credit on human rights due diligence for publishing a risk assessment on the impact of Russian law on user privacy (G4).[4] Yandex also disclosed a grievance mechanism for users to file complaints about content removed for alleged copyright infringements but not about content removed for terms of service violations (G6).[5]

FREEDOM OF EXPRESSION 23%

Yandex ranked seventh out of the 12 internet and mobile companies evaluated in the Freedom of Expression category, ahead of Apple, Tencent, Mail.Ru, and Baidu.

Content and account restrictions: Yandex disclosed little about how it enforces its terms of service (F3, F4, F8), although it had a similar level of disclosure as Apple and Mail.Ru. Yandex Search provided the most detailed disclosure about prohibited content of the three services evaluated (F3). However, Yandex did not publish any data about content or accounts the company restricts for violating its own rules (F4), and did not make clear whether it notifies users when content or their account has been restricted (F8).

Content and account restriction requests: Yandex also had weak disclosure about how it handles government and private requests to restrict content or accounts (F5, F6, F7), although it outperforms Apple, Mail.Ru, Tencent, Baidu, and Samsung on these indicators. The company did not clearly disclose its process for responding to government and third-party requests for account restrictions (F5), nor did it publish any data on the number of government requests it receives or complies with (F6). Yandex stood out for being among just a few companies—including top-performing Google, Yahoo, Microsoft and Twitter—that disclosed any information about compliance with private requests to remove content in response to Russia's new "Right to be Forgotten" law.[6]

Identity policy: Yandex disclosed it can ask users to confirm their offline identity, and may deny access to services to users who do not comply (F11), although it is not explicitly required to do so by law.

PRIVACY 37%

Yandex ranked eighth out of the 12 internet and mobile companies evaluated in the Privacy category, ahead of Mail.Ru, Samsung, Tencent, and Baidu.

Handling of user information: Yandex disclosed more than Mail.Ru, Samsung, and Baidu about how it handles user information but there is much room for improvement. It provided some evidence about what user information it collects (P3), shares (P4), and why (P5) but did not reveal how long it retains user information (P6)—although it is not illegal to do so. Nor did it disclose if users can access the information the company holds about them (P8), or what information the company collects about about users from third parties (P9).

Requests for user information: Yandex disclosed little about its process for responding to government or private requests for user information (P10) and supplied no data about requests it receives or complies with (P11). However, since Russian authorities may have direct access to communications data through SORM, Russian companies may not be aware of the frequency or scope of user information accessed by authorities.

Security: Yandex was one of the top-performing companies on these indicators, behind only Google (P13-P18). It disclosed a particularly strong bug bounty program (P14). But like most companies, Yandex provided no information about how it responds to data breaches (P15). The company, however, received the second-highest score after Google for its disclosure more about it encryption policies, on par with Apple (P16). It disclosed that the transmissions of users' communications are encrypted by default and with unique keys.

[4] "Form 20-F, Annual Report 2015 - Yandex" (United States Securities and Exchange Commission, March 22, 2016),
[5] "On the Responsibility of Users and Complaints about Content," **http://yandex.ru/support/common/support/complaints-about.html**.
[6] "On Amendments to the Federal Law 'On Information, Information Technologies and Protection of Information' and Articles 29 and 402 of the Civil Procedure Code of the Russian Federation," Federal Law 264-FZ (2015).

AMÉRICA MÓVIL, S.A.B. DE C.V.

● **Telecommunications Company**

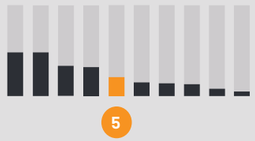
Key Findings:

- América Móvil lacked clear disclosure of policies that affect users' freedom of expression and privacy.
- The company lacked disclosure of how it handles government and private requests to restrict content or accounts, or to hand over user information.
- Without changes to the law, the company could improve its disclosure in several areas, including by publishing transparency reports in keeping with its industry peers.

OVERALL SCORE

21%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

TELCEL

Mexico

SERVICES EVALUATED

- Pre-Paid Mobile
- Post-Paid Mobile

ANALYSIS

América Móvil ranked fifth out of the 10 telecommunications companies evaluated and 16th in the Index overall.[1] Although Freedom House rates Mexico's internet environment as "Partly Free," the company could improve its disclosure on a number of policies even if laws and regulations do not change.[2] These include the company's policies on network management and data retention. There is no obstacle in Mexico to reporting the number of government and private requests the company receives to share user information (P11). Mexico's telecommunications authority requires companies to report on the number of government requests for real-time location tracking or access to user metadata, but the company has not published this data.[3] Notably, the company's disclosure about its security oversight improved since the 2015 Index, as its 2015 Sustainability Report included more detail about its internal systems to monitor employee access to information.[4]

About América Móvil, S.A.B. de C.V.

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

Market Cap: USD 43,093 million[5]
BMV: AMX L
Domicile: Mexico
Website: www.americamovil.com

[1] For América Móvil's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/americamovil.**
[2] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/mexico.**
[2] "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).
[3] "2015 Sustainability Report," America Movil, **http://www.americamovil.com/sites/default/files/2016-09/AMX-IS-2015-ingles.pdf.**
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 21%

América Móvil ranked 13th of all 22 companies evaluated in the Governance category. Although América Móvil committed to protect users' privacy, it fell short of articulating its commitment to privacy as part of a broader commitment to human rights (G1).[5] The company lacked clear disclosure across a number of indicators, including whether it conducts human rights impact assessments (G4) or if it engages with a range of stakeholders on freedom of expression and privacy issues (G5). América Móvil, however, tied with Etisalat for the second-highest score of all 22 companies, after Vodafone and Bharti Airtel, for its disclosure of a grievance mechanism, including statistics for the number of privacy complaints it received (G6).

FREEDOM OF EXPRESSION 16%

América Móvil ranked fourth among telecommunications companies in the Freedom of Expression category, after Vodafone, AT&T, and Telefónica but on par with Orange.

Content and account restriction requests: América Móvil's operating company Telcel lacked disclosure of how it handles or complies with government and third-party requests to restrict content or user accounts. It was one of six telecommunications companies evaluated to score no points on these indicators (F5-F7).

Network management and shutdowns: Telcel disclosed little about its network management and shutdown policies, like most telecommunications companies evaluated (F9, F10). Despite committing to net neutrality, Telcel stated it offers zero rating for certain content on specific social networks and instant messaging services (F9). The company did not disclose any information about how it handles or responds to network shutdown requests (F10).

Identity policy: The company did not clearly disclose if pre-paid mobile users need to provide a government-issued identification—and there is no law in Mexico requiring companies to do so. The Telcel pre-paid mobile contract asked users to provide their identification, although it was not clear if this is mandatory. In practice it may be possible for users to purchase a prepaid SIM card without providing identification but this was not clearly specified (F11).

PRIVACY 24%

América Móvil ranked fifth out of the 10 telecommunications companies evaluated in the Privacy category.

Handling of user information: While América Móvil's Telcel disclosed less about how it handles user information compared to Vodafone and AT&T, it performed better than most other telecommunications companies on this set of indicators, on par with Orange and Telefónica (P3-P8). The company disclosed little about what types of user information it collects (P3), shares (P4), and why (P5). Like all telecommunications companies but AT&T, Telcel provided no disclosure of how long it retains user information (P6), although no law prohibits the company from doing so.[6]

Requests for user information: Like most telecommunications companies, Telcel provided almost no information about how it handles requests from governments and private parties to share user information (P10-P11). The company 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.

Security: Telcel did not provide as much information about its security policies as AT&T, Telefónica, and Vodafone, but outperformed the rest of the telecommunications companies on these indicators (P13-P18). The company disclosed more about its security oversight since the 2015 evaluation, including more detail about its internal systems to monitor employee access to information (P13). Like most companies in the Index, Telcel disclosed nothing about how it responds to data breaches (P15). Companies are legally required to notify users only if the data breach "significantly affects" their rights.[7]

[5] "2015 Sustainability Report," América Móvil.
[6] "Federal Telecommnications and Broadcasting Law" (2014).
[7] "Ley Federal de Protección de Datos Personales En Posesión de Los Particulares," Article 20 (2010).

AT&T, INC.

● Telecommunications Company

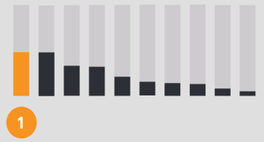
Key Findings:

- AT&T tied with Vodafone as the top-ranked telecommunications company in the 2017 Index.
- AT&T had notably weaker disclosure of policies related to network management and network shutdowns in comparison to Vodafone.
- While AT&T received top marks for disclosing how it secures user information, it should be more transparent about what user information it collects, shares, and retains.

OVERALL SCORE

48%

TELECOMMUNICATIONS RANK



SERVICES EVALUATED

- **Pre-Paid Mobile**
- **Post-Paid Mobile**
- **Fixed-Line Broadband**

ANALYSIS

AT&T tied with Vodafone as the top-ranked telecommunications company of the 2017 Index.[1] A member of the Telecommunications Industry Dialogue (TID), AT&T made notable improvements in 2016, including conducting a human rights impact assessment of its operations in Mexico, and clarifying of its process for handling private requests for content and account restrictions and user information. Notably, AT&T made strong commitments to freedom of expression and privacy as human rights at the corporate level. However, it had weaker disclosure of actual policies that affect users' freedom of expression and privacy in practice—as demonstrated by its higher scores in the Governance category as compared to its performance in other Index categories. Nonetheless, AT&T disclosed more about its policies and practices that affect users' freedom of expression and privacy than all other telecommunications companies evaluated, apart from Vodafone. However, new information about Hemisphere, a warrantless surveillance tool created by AT&T and marketed to U.S. law enforcement, raises questions about the company's commitment to users' privacy in practice.[2]

About AT&T, Inc.

AT&T, Inc. provides telecommunications services in the United States and internationally. In 2015, the company expanded its operations to Mexico after purchasing two Mexican telecommunications companies. The company offers data and voice services to approximately 144 million wireless subscribers in the U.S. and Mexico.[3]

Market Cap: USD 254,032 million[4]
NYSE: T
Domicile: United States
Website:www.att.com

[1] For AT&T's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/att**.
[2] Kenneth Lipp, "AT&T Is Spying on Americans for Profit, New Documents Reveal," *The Daily Beast*, October 25, 2016.
[3] "3Q 2016 AT&T by the Numbers," **https://www.att.com/Common/about_us/pdf/att_btn.pdf.**
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 67%

AT&T received the third-highest score in the Governance category among telecommunications companies, behind Vodafone and Orange, and the fifth-highest score of all 22 companies evaluated. AT&T publicly committed to respect human rights, including freedom of expression and privacy (G1), and provided evidence of senior-level oversight over these issues (G2). AT&T also disclosed it conducted a human rights impact assessment (HRIA) after expanding into Mexico.[5] However, since the HRIA was conducted after AT&T had already entered the market, it received partial credit (G4). AT&T had the fourth-highest score among telecommunications companies on disclosure of grievance and remedy mechanisms (G6). It did not disclose a company-wide grievance mechanism that includes freedom of expression concerns, and aside from its policies on responding to copyright counter-notices, did not reveal its process for responding to freedom of expression or privacy complaints.

FREEDOM OF EXPRESSION 41%

AT&T was the second-best scoring telecommunications company in the Freedom of Expression category, behind Vodafone.

Content and account restriction requests: AT&T was one of only four telecommunications companies to receive any credit for disclosing its handling of government and private requests to restrict content or accounts (F5-F7). Notably, AT&T was one of two telecommunications companies to receive any credit for publishing data on government requests to restrict content or user accounts (F6). The company improved its disclosures since 2015 by clarifying it does not entertain private requests.

Network management and shutdowns: AT&T disclosed less information than Vodafone on its policies related to network management and shutdowns, but more than most telecommunications companies evaluated. While the company revealed reasons it may engage in network management practices, it did not clearly indicate it will not engage in content blocking/prioritization practices (F9). AT&T provided minimal disclosure on its policies related to network shutdowns (F10). It is unclear whether there are any legal factors prohibiting AT&T from disclosing more about its network shutdown policies, as the U.S. government's policy on network shutdowns is secret.[6]

Identity policy: AT&T did not disclose that it requires prepaid mobile service users to verify their identity with a government issued ID, making it one of only two telecommunications companies evaluated to receive full credit on this indicator (F11).

PRIVACY 47%

AT&T was the highest-scoring telecommunications company in the Privacy category.

Handling of user information: AT&T disclosed more than all other telecommunications companies apart from Vodafone about how it handles user information (P3-P8). Still, it did not fully disclose what types of user information it collects (P3), shares (P4), and why (P5). The company revealed even less information about how long it retains this information (P6), although it was the only telecommunications company to score any points on this indicator. AT&T had a similar level of disclosure as Vodafone on how users can control what information about them is collected and shared (P7) but lagged behind Vodafone on disclosure of users' ability to obtain all of the information a company holds on them (P8).

Requests for user information: AT&T received the highest score of all telecommunications companies for its disclosure of its process for responding to and complying with government and private requests for user information (P10, P11). AT&T did not indicate whether it notifies users about requests for their information (P12).

Security: AT&T disclosed more than all telecommunications companies about its security policies and was the only one of its peers to receive full credit for disclosure about its internal processes for ensuring that user data is secure (P13). AT&T was also one of only three companies in the entire Index to reveal any information about how it handles data breaches, although its disclosure still fell short (P15).

[5] "AT&T's Commitment to Freedom of Expression and Privacy," (January 2017) **https://about.att.com/content/dam/csr/PDFs/ATT_Industry_Dialogue_Reporting_Matrix.pdf**.
[6] Electronic Privacy Information Center, "EPIC v. DHS - SOP 303," **http://epic.org/foia/dhs/internet-kill-switch/**.

AXIATA GROUP BERHARD

● **Telecommunications Company**

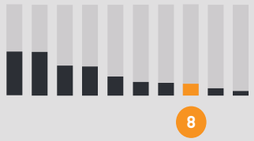
Key Findings:

- Axiata does not commit to respect human rights and has insufficient disclosure of policies affecting users' freedom of expression and privacy.
- The company offered minimal information about its process for handling network shutdowns.
- Axiata revealed no information about its process for responding to requests from governments or private parties to block content or user accounts, or to hand over user information. There are no legal factors preventing it from disclosing at least some of this information.

OVERALL SCORE

13%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

CELCOM

Malaysia

SERVICES EVALUATED

- **Pre-Paid Mobile**
- **Post-Paid Mobile**

ANALYSIS

Axiata ranked eighth out of the 10 telecommunications companies evaluated and 19th in the Index overall.[1] The 2016 *Freedom on the Net* report by Freedom House rated Malaysia's internet environment as "Partly Free."[2] Celcom, Axiata's operating company in Malaysia, is subject to orders and instructions from the Malaysian Communications and Multimedia Commission (MCMC) and other authorities—many of which are not published or otherwise available to the public. However, there are no laws prohibiting Axiata from making basic commitments to respect users' rights to free expression and privacy. Axiata could, for instance, improve its disclosure of how it handles government and private requests for 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 third-party requests for user information.[3]

About Axiata Group Berhad

Axiata Group Berhad provides various telecommunication and network transmission-related services to numerous markets across Asia under various brand names. The company has almost 300 million mobile subscribers in Asia.[4] It operates primarily under the brands of Celcom in Malaysia, XL in Indonesia, Dialog in Sri Lanka, Robi in Bangladesh, Smart in Cambodia, Idea in India, and M1 in Singapore.

Market Cap: USD 10,178 million[5]
KLSE: AXIATA
Domicile: Malaysia
Website:www.axiata.com

[1] For Axiata's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/axiata**.
[2] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/malaysia**.
[3] "Official Secrets Act 1972," Act 88 (1972).
[4] "Key Highlights," Axiata Group Berhad, accessed February 17, 2017, **https://www.axiata.com/corporate/key-highlights/**.
[5] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 3%

Axiata received the third-lowest score of all companies evaluated in the Governance category, scoring higher than only Ooredoo and Baidu. In this category, Axiata received some credit on only one indicator (G2) for disclosing that its board of directors oversees privacy issues across all of the group's operating companies.

FREEDOM OF EXPRESSION 13%

Axiata received the second-lowest score among telecommunications companies in the Freedom of Expression category, on par with MTN, and ahead of only Bharti Airtel.

Content and account restriction requests: Like most of its peers, Axiata's Malaysian subsidiary Celcom did not clearly disclose information about how it handles or complies with government and other third-party requests to restrict content or accounts (F5-F7). Celcom did not provide any disclosure on its process for responding to third-party requests for content or account restriction (F5), or publish data about the number of these types of requests it receives or complies with (F6, F7).

Network management and shutdowns: Like most telecommunications companies, 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 (F9), but had minimal disclosure of why it may shut down access to the network for a user or group of users (F10).

Identity policy: The Malaysian government requires telecommunications companies to register pre-paid SIM cards with a user's identity card or passport.[6] Celcom pre-paid mobile users are therefore required to provide their identification (F11).

PRIVACY 18%

Axiata placed sixth out of the 10 telecommunications companies evaluated in the Privacy category, ahead of Bharti Airtel, MTN, Etisalat, and Ooredoo.

Handling of user information: While Celcom disclosed less information than most other telecommunications companies on these indicators, it performed better than MTN, Etisalat, and Ooredoo (P3-P8). Celcom only partially disclosed what user information it collects, shares and why (P3, P4, P5) and—like most telecommunications companies other than AT&T—provided no information about how long it retains user information (P6). Celcom also offered users no information about how they can control what information the company collects about them or options to obtain this information (P7, P8). The Malaysian Personal Data Protection Act (PDPA) states that personal data processed for any purpose should not be kept longer than is necessary for the fulfillment of that purpose; it does not prevent companies from fully disclosing the information addressed by these indicators.[7]

Requests for user information: Axiata, Etisalat, and Ooredoo were the only three telecommunications companies to receive no credit on these indicators (P10-P12). Celcom did not reveal its processes for responding to government and private requests for user information or publish data on the volume and nature of these requests it receives or complies with (P10, P11). Celcom also did not commit to notify users if their information has been requested by a government or other type of third party (P12). The country's Official Secrets Act should not prevent the company from disclosing its process for responding to government and other third-party requests for share user information.

Security: Celcom disclosed little information about its security policies, scoring better than only MTN, Etisalat, and Ooredoo on these indicators (P13-P18). It offered some information about its internal security policies, such as limiting and monitoring employee access to user information (P13), but did not disclose policies for addressing security vulnerabilities (P14) or for responding to data breaches (P15).

[6] "Prepaid Registration Exercise in Malaysia" (Malaysian Communications and Multimedia Commission). **http://www.skmm.gov.my/skmmgovmy/files/attachments/Info-updated%204July06.pdf**.
[7] "Personal Data Protection Act 2010," Act 709 (2010),

BHARTI AIRTEL LIMITED

● Telecommunications Company

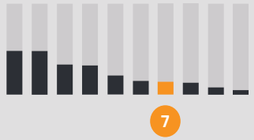
Key Findings:

- Bharti Airtel's weak commitments and disclosures related to freedom of expression and privacy could be significantly improved even without any changes being made to India's laws and regulations.
- Bharti Airtel's lack of disclosure about policies related to network shutdowns is of particular concern given that as many as 30 government-ordered internet shutdowns occurred in India in 2016.[1]
- The company led its telecommunications peers in offering grievance and remedy mechanisms due to the requirements of Indian law.

OVERALL SCORE

14%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

AIRTEL INDIA

India

SERVICES EVALUATED

- **Pre-Paid Mobile**
- **Post-Paid Mobile**
- **Fixed-Line Broadband**

ANALYSIS

Bharti Airtel ranked seventh out of the 10 telecommunications companies evaluated and 18th in the Index overall.[2] In 2016, Freedom House rated the internet environment in India as "partly free," citing the growing frequency of internet shutdowns around the country as a threat to internet users' rights.[3] While Bharti Airtel has a corporate social responsibility program that stresses the importance of a "responsible business approach" addressing "every dimension of how business operates in the social, cultural, and economic environment,"[4] the company demonstrated weak respect for users' freedom of expression and privacy rights.

About Bharti Airtel Limited

Bharti Airtel Limited provides telecommunication systems and services worldwide, including in India, South Asia, and Africa. The group delivers a variety of fixed and mobile voice and data telecommunications services across these markets.

Market Cap: USD 21,343 million[5]
BSE: 532454
Domicile: India
Website:www.airtel.in

[1] "Internet Shutdowns in India," Accessed February 16, 2017, **http://internetshutdowns.in**.
[2] For Bharti Airtel's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/bhartiairtel**.
[3] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/india**.
[4] "Sustainability," Airtel India, accessed February 16, 2017, **http://www.airtel.in/sustainability-file/home.html**.
[5] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 16%

Bharti Airtel performed poorly in the Governance category, placing in the bottom half of all companies evaluated. India's legal environment does not prevent the company from making commitments to respect freedom of expression and privacy in its operating markets (G1), from establishing senior-level oversight over how the company handles freedom of expression and privacy issues (G2), or from creating a process for human rights due diligence (G4). The company received partial credit for Airtel India's stakeholder engagement but there is no evidence of stakeholder engagement in other markets (G5). Notably, Bharti Airtel tied for first place with Vodafone for grievance and remedy mechanisms (G6). Indian law requires service providers to have grievance officers and redress mechanisms.[6]

FREEDOM OF EXPRESSION 10%

As in the 2015 Index, Bharti Airtel earned the lowest score in the Freedom of Expression category of any telecommunications company.

Content and account restriction requests: Like most telecommunications companies evaluated, Airtel India disclosed nothing about how it handles government and private requests it receives to restrict content or user accounts (F5-F7). Indian law forbids disclosure of government requests to block content, but nothing prevents companies from disclosing their process for handling these types of requests, or from having a clear policy of notifying users when they restrict or block content they publish, transmit, or attempt to access (F8).

Network management and shutdowns: As a result of legal requirements, Airtel India disclosed more information than most of its peers about its network management policies (F9), earning it the third highest score on this indicator. However, the company disclosed little about its policies and practices related to network shutdowns. 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 (F10).

Identity policy: Airtel India disclosed that it requires pre-paid mobile users to provide a government-issued identification, which is also required by law (F11).[7]

PRIVACY 17%

Bharti Airtel placed seventh out of the 10 telecommunications companies in the Privacy category.

Handling of user information: Airtel India disclosed less than most telecommunications companies about how it handles government and private requests for user information, though it performed better than MTN, Etisalat, and Ooredoo on these indicators (P3-P8). Airtel India offered some disclosure of what types of user information it collects, shares, and why (P3, P4, P5), but did not disclose how long it retains this information (P6). Nor did it disclose whether it enables users to control what information about them is collected and shared, or to obtain the information the company holds about them (P7, P8).

Requests for user information: Like most telecommunications companies, Airtel India disclosed little about how it handles government and private requests for user information (P10-P11). Indian law prevents companies from reporting data on government requests but does not prevent them from disclosing their process for responding to different types of third-party requests for user information.

Security: Airtel India scored above the telecommunications company average on these indicators (P13-P18). But it offered no information about its efforts to address vulnerabilities (P14) and was silent about its process for responding to data breaches (P15). More positively, the company did win full points for its efforts to educate users about security threats (P18).

[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),
[7] "Subscriber Verification," Department of Telecommunications, **http://www.dot.gov.in/access-services/subscriber-verification**.

ETISALAT GROUP

● Telecommunications Company

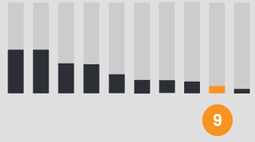
Key Findings:

- Etisalat made no commitment to respect human rights and disclosed little about policies affecting users' freedom of expression and privacy.
- The company disclosed no information about how it handles government and private requests to restrict content or accounts, or for user information.
- Despite legal constraints on companies in the UAE, Etisalat should make its privacy policies available to users and provide more information about what the company does to keep user information secure.

OVERALL SCORE

8%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

ETISALAT UAE

United Arab Emirates

SERVICES EVALUATED

- Pre-Paid Mobile
- Post-Paid Mobile
- Fixed-Line Broadband

ANALYSIS

Etisalat ranked ninth out of the 10 telecommunications companies evaluated and received the second-lowest score in the Index overall.[1] Etisalat is a majority state-owned company,[2] operating in a political and regulatory environment not conducive to companies making public commitments to human rights, including to freedom of expression and privacy. The 2016 *Freedom on the Net* report by Freedom House rated the UAE's internet environment as "Not Free."[3] However, Etisalat could still improve its disclosures dispite these constraints. For example, it could clarify which privacy policy applies to its services. In addition, the company disclosed nothing about how it responds to government and private requests for user information. Given that the company is majority state-owned and that the overall operating environment discourages transparency—and in some cases, such as for police investigations or court trials, legally prohibits it—it is unlikely Etisalat would be able to disclose this information about government requests. However, it could disclose its processes for receiving and complying with private requests for content restriction or user information. It could also provide more information about its security policies, as there is no law for instance prohibiting companies from disclosing their process for responding to data breaches.

About Etisalat Group

Etisalat Group establishes and operates telecommunication and fiber optics networks, along with a broad suite of other services in the United Arab Emirates and in 16 other countries in the Middle East, Africa, and Asia. Its operations include operation and management of telecom networks as well as media services, connectivity services, and consulting.

Market Cap: USD 42,622 million[4]
ADX: ETISALAT
Domicile: United Arab Emirates (UAE)
Website:www.etisalat.com

[1] For Etisalat's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/etisalat**.
[2] "Investor Relations - Investor Relations," Etisalat, accessed February 17, 2017, **http://www.etisalat.com/en/ir/corporateinfo/overview.jsp**.
[3] "Freedom on the Net" (Freedom House, November 2016), **https://freedomhouse.org/report/freedom-net/2016/united-arab-emirates**.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 8%

Etisalat performed poorly in the Governance category, receiving the fifth-lowest score of all 22 companies, ahead of Mail.Ru, Axiata, Ooredoo, and Baidu.

Etisalat provided no formal commitment to respect users' freedom of expression and privacy as human rights (G1), and disclosed no senior-level oversight over these issues (G2).

The company revealed no evidence of a human rights due diligence process (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 relating to free expression or privacy (G6).

FREEDOM OF EXPRESSION 15%

Etisalat ranked sixth out of the 10 telecommunications companies evaluated in the Freedom of Expression category, ahead of Ooredoo, MTN, Axiata, and Bharti Airtel.

Content and account restriction requests: Like most telecommunications companies evaluated, Etisalat UAE provided almost no information about how it handles government or private requests to restrict content or accounts (F5-F7). For fixed-line broadband services, the company stated that it reviews users' requests to block or unblock internet content under the UAE's "Internet Access Management Policy," which prohibits certain types of content, but provided no additional information about how it responds to content-blocking or account restriction requests for its mobile services (F5).[5] Likewise, Etisalat did not publish any data about government or private requests to restrict content or accounts that it receives or complies with (F6, F7).

Network management and shutdowns: Etisalat UAE was among the lowest-scoring companies on these indicators, though it offered slightly more disclosure than Ooredoo (F9-F10). Etisalat failed to disclose any information about its network management policies (F9) and had only vague disclosure of policies related to network shutdowns (F10).

Identity policy: Etisalat UAE disclosed that it requires pre-paid mobile service users to provide government-issued identification (F11). The UAE Telecom Regulatory Authority (TRA) requires all mobile phone service subscribers to do so.[6]

PRIVACY 2%

Etisalat received the second-lowest score of the 10 telecommunications companies evaluated in the Privacy category, slightly ahead of Ooredoo.

Handling of user information: Etisalat UAE disclosed almost nothing on these of indicators, scoring better than only Ooredoo (P3-P8). The company's privacy policy referred only to the Etisalat UAE website and online services with no indication of whether this policy applies to mobile or fixed-line broadband services.[7] It therefore received no credit on indicators addressing company disclosure of what types of user information it collects, for what purpose, and for how long it retains it (P3, P5, P6). The company did, however, receive some credit for disclosing that it shares user information with authorities if legally required and in cases of national security (P4).

Requests for user information: Etisalat UAE did not provide any information about how it handles requests for user information from governments and private parties, making it one of three companies, along with Ooredoo and Axiata, that received no credit on these indicators (P10-P11).

Security: Etisalat UAE had almost no disclosure on these indicators, scoring better than only Ooredoo (P13-P18). It disclosed that it has policies in place limiting employee access to user data but provided no additional information regarding its internal processes for ensuring that user data is secure (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.

[5] "Blocking and Unblocking Internet Content," Etisalat, **http://www.etisalat.ae/en/aboutus/corporate/blocking-unblocking.jsp**.
[6] "TRA Links Mobile Registration with 'ID Card,'" Emirates Identity Authority, February 9, 2015, **http://www.id.gov.ae/en/media-centre/news/2014/2/9/tra-links-mobile-registration-with-id-card.aspx**.
[7] "Privacy Policy - General terms of use for the website and Etisalat's online services," Etisalat, May 24, 2015, **http://www.etisalat.ae/en/generic/privacy-policy.jsp**.

MTN GROUP LIMITED

● Telecommunications Company

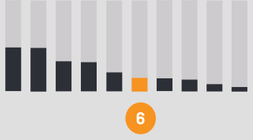
Key Findings:

- MTN made a commitment to human rights at the corporate level, but lacked disclosure of policies that affect users' freedom of expression and privacy in practice.
- MTN disclosed almost no information about how it handles government or private requests to restrict content or accounts, or for user information. South African law prevents disclosure of government requests for user information, but MTN could disclose government requests for content restrictions and requests from private parties.
- MTN revealed little about how it secures user information, including how it responds to data breaches.

OVERALL SCORE

15%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

MTN SOUTH AFRICA

South Africa

SERVICES EVALUATED

- Pre-Paid Mobile
- Post-Paid Mobile

ANALYSIS

MTN ranked sixth out of the 10 telecommunications companies evaluated and 17th in the Index overall.[1] Although South Africa's internet environment is ranked as "free" by Freedom House,[2] the company operates in a number of challenging markets including Iran, Rwanda, Afghanistan, and other countries across the Middle East and North Africa, making it difficult for the company to disclose concrete policies to implement its commitment to respect human rights across all of its global operations. MTN's group-level corporate entity has historically relied on the company's operations outside of South Africa for revenue. While South African law might prevent some specific disclosures, it does not prevent MTN South Africa from being much more transparent in general about policies and practices that affect users' freedom of expression and privacy.

About MTN Group Limited

MTN Group Limited is a telecommunications company that serves markets in more than 20 countries in Africa, Asia, 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 16,398 million[4]
JSE: MTN
Domicile: South Africa
Website: www.mtn.com

[1] For MTN's performance in the 2015 Index, see: https://rankingdigitalrights.org/index2015/companies/mtn.
[2] "Freedom on the Net" (Freedom House, November 2016), https://freedomhouse.org/report/freedom-net/2016/south-africa.
[3] "Where We Are," MTN Group, accessed February 20, 2017, https://www.mtn.com/en/mtn-group/about-us/our-story/Pages/where-we-are.aspx.
[4] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 31%

MTN received the ninth-highest score of all 22 companies evaluated in the Governance category, and notably, ahead of Twitter and Apple. The company disclosed an explicit commitment to freedom of expression and privacy as human rights (G1)[5] and evidence of senior-level oversight over these issues within the company (G2). However, the company fell short on the remaining governance indicators: it disclosed a whistleblower program, but the focus of the program appeared related only to corruption and fraud (G3).[6] Although MTN noted plans to finalize internal risk assessment guidelines, it did not reveal if it currently engages in human rights due diligence practices (G4).[7] Likewise, MTN lacked clear disclosure of whether it engages with stakeholders on freedom of expression and privacy issues (G5), or of a grievance and remedy mechanism allowing users to address freedom of expression and privacy concerns (G6).

FREEDOM OF EXPRESSION 13%

In the Freedom of Expression category, MTN tied with Axiata for the second-lowest score of all telecommunications companies, ahead of Bharti Airtel.

Content and account restriction requests: MTN was one of the six telecommunications companies to receive no credit on these indicators (F5-F7). The company did not clearly disclose its process for handling government or private requests to restrict content or accounts (F5), nor did it publish any data about the number of such requests it received or complied with (F6, F7). South African law does not prevent companies from disclosing this information.

Network management and shutdowns: MTN disclosed little about its network management and shutdown policies (F9, F10). The company enables users to access Facebook without charging their data plan, a practice known as "zero rating," but disclosed nothing more about its network management practices (F9). MTN also provided minimal information about its network shutdown policies and procedures (F10).

Identity policy: MTN South Africa disclosed that users must register their SIM card with the company using their government-issued identification. All mobile phone users in South Africa are legally required to do so (F11).[5]

PRIVACY 11%

MTN ranked eighth out of the 10 telecommunications companies in the Privacy category, ahead of only Etisalat and Ooredoo.

Handling of user information: MTN was among the lowest-scoring companies on these indicators, offering slightly more disclosure than Etisalat and Ooredoo (P3-P8). It provided just minimal information about what types of user information it collects and why (P3, P5), but no information about what it shares or for how long it retains user information (P4, P6). The company also failed to disclose options users have to control what information about them the company collects and shares (P7), or to obtain all of the information the company holds on them (P8).

Requests for user information: Like most telecommunications companies, MTN provided almost no information about how it handles requests from governments and private parties for user information (P10-P11). It gave little information about its process for handling such requests (P10) and no data about the number of such requests it receives or complies with (P11). Companies in South Africa are prohibited from publishing such information about government requests, including the fact that a request was made, but nothing prevents them from fully disclosing how they handle private requests and the number of these requests they receive and comply with.

Security: MTN had low disclosure on this set of indicators, scoring better than only Etisalat and Ooredoo (P13-P18). The company revealed that it conducts audits to address security vulnerabilities, but did not clearly disclose whether it has a security team that conducts these audits (P13). However, it was one of only two telecommunications companies to offer any disclosure on its processes for addressing security vulnerabilities (P14). Like most companies, MTN offered no information about how it handles data breaches (P15).

[5] "Regulation Of Interception Of Communications And Provision Of Communication-Related Information Act," Pub. L. No. Act No. 70 (2002).

OOREDOO Q.S.C.

● Telecommunications Company

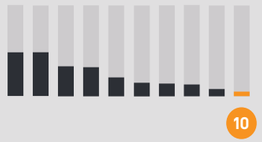
Key Findings:

- Ooredoo made no public commitment to respect human rights and failed to disclose sufficient information about policies affecting users' freedom of expression and privacy.
- Ooredoo, which is majority owned by the Qatari government, revealed no information about what user information it collects, shares, or retains, or how it handles or complies with government or private requests for this information.
- The company disclosed no information about what measures it takes to secure user information, including any policies related to data breaches.

OVERALL SCORE

5%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

OOREDOO QATAR

Qatar

SERVICES EVALUATED

- Pre-Paid Mobile
- Post-Paid Mobile
- Fixed-Line Broadband

ANALYSIS

A new addition to the Index, Ooredoo received the lowest score of any company evaluated this year. The political and regulatory environment in Qatar is not conducive to companies making public commitments to human rights, including to freedom of expression and privacy. Ooredoo is majority owned by the government.[1] According to Amnesty International, freedom of expression is "strictly controlled" in Qatar.[2] Under its cybercrime law users may be punished for posting or sharing online content that violates Qatar's "social values."[3] However, Ooredoo could still significantly improve its public disclosures even within such constraints. The company could clearly disclose its privacy policies and provide basic information about its security practices, including how it handles data breaches. Qatar passed its first comprehensive data privacy law in 2016, which requires companies to take steps that "protect personal data from loss, damage, modification, disclosure or being illegally accessed" and notify the government and users in the event of a data breach.[4]

About Ooredoo Q.S.C.

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. Formerly known as Qatar Telecom (Qtel), the company changed its name in 2013. It also provides services including satellite and data center solutions.

Market Cap: USD 9,360 million[5]
DSM: ORDS
Domicile: Qatar
Website: www.ooredoo.qa

[1] "Share Information," Ooredoo Corporate, accessed February 20, 2017, http://ooredoo.com/en/investors/share_information/.
[2] "Qatar: Blocking of Doha News Website 'an Outright Attack' on Media Freedom," Amnesty International, December 1, 2016, https://www.amnesty.org/en/latest/news/2016/12/qatar-blocking-of-doha-news-website-is-an-outright-attack-on-media-freedom/.
[3] "WhatsApp Insults Lead to Jail Sentence for Qatar Woman," Doha News, November 25, 2015, https://dohanews.co/whatsapp-insults-leads-to-jail-sentence-for-qatar-woman/.
[4] "New Law on Personal Data Protection," Qatar Tribune, November 4, 2016, http://www.qatar-tribune.com/news-details/id/31687.
[5] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 2%

Ooredoo performed poorly in the Governance category, receiving the lowest score of all telecommunications companies and second-lowest score in the entire Index. Ooredoo offered no public commitment to freedom of expression and privacy as human rights (G1), nor did it disclose having senior-level oversight over these issues (G2). Although it disclosed a whistleblower policy, the policy did not mention if it covers freedom of expression or privacy issues (G3). The company also offered no evidence that it has any human rights due diligence processes in place (G4), or if it engaged with stakeholders on freedom of expression or privacy issues (G5). Ooredoo Qatar provided some disclosure of how customers may submit complaints, but there was no additional information about its processes for receiving and responding to such grievances (G6).

FREEDOM OF EXPRESSION 14%

Ooredoo performed poorly in the Freedom of Expression category, receiving the third-lowest score among telecommunications companies, and scoring just slightly better than MTN, Axiata, and Bharti Airtel.

Content and account restriction requests: Ooredoo, like most of its peers, received no credit on these indicators (F5-F7). It 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 receives or complies with (F6, F7), although 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 from a general lack of transparency in the Qatari legal environment.

Network management and shutdowns: Ooredoo did not disclose any information about its network management policies (F9). The company provided vague disclosure on why it may shut down service to an area or particular group of users, but did not disclose any other information on its processes related to government requests for network shutdowns (F10).[6]

Identity policy: Ooredoo Qatar disclosed that it requires pre-paid mobile users to provide government-issued identification (F11), although it is unclear if this is required by law.

PRIVACY 0%

Ooredoo received the lowest score among telecommunications companies in the Privacy category, and was the only company evaluated in the Index to receive no credit for any privacy indicator.

Handling of user information: Ooredoo was the only company in the entire Index to provide no disclosure across this set of indicators (P3-P8). The company's privacy policy was not publicly available. The privacy policy that was available online for Ooredoo Qatar only covers the website.

Requests for user information: Ooredoo, Etisalat, and Axiata were the only three telecommunications companies to receive no credit across these indicators (P10-P12). Ooredoo did not disclose any information about its process for responding to government or private third party requests for user information (P10) including whether it notifies users when such parties request their information (P12). The company also did not publish any data about the number of requests it receives for user information (P11).

Security: Ooredoo was the only company in the entire Index to provide no disclosure across this set of indicators (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).

[6] "General Terms and Conditions for Consumer Services," https://www.ooredoo.qa/portal/OoredooQatar/general-terms-and-conditions

ORANGE

● Telecommunications Company

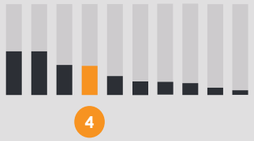
Key Findings:

- Orange made strong public commitments to freedom of expression and privacy at the governance level, but revealed less about its policies affecting these rights in practice.
- Orange offered no information about how it handles or complies with government and other third-party requests to restrict content or accounts.
- The company should clarify its policies and practices regarding network shutdowns and disclose more about how it handles user information.

OVERALL SCORE

32%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

ORANGE FRANCE

France

SERVICES EVALUATED

- Pre-Paid Mobile
- Post-Paid Mobile
- Fixed-Line Broadband

ANALYSIS

Orange ranked fourth out of the 10 telecommunications companies evaluated and 11th in the Index overall.[1] A member of the Telecommunications Industry Dialogue (TID), Orange disclosed strong public commitments to freedom of expression and privacy as human rights at the governance level, but revealed far less about its policies affecting these rights in practice. Like all companies, Orange is constrained by legal requirements in the countries where it operates, including in France, but there are changes it can make that would not necessitate legal reform. For instance, French intelligence services have permanent, unchecked access to Orange's network,[2] and the company could be more upfront with users about the state's surveillance powers. It could also significantly improve its disclosure of network shutdown policies, as there is no apparent legal obstacle to doing so.

About Orange

Orange provides a range of fixed telephony and mobile telecommunications, data transmission, and other value-added services to consumers, businesses, and other telecommunications operators worldwide with a major presence in Europe and Africa. The company offers mobile, fixed-line, and carrier services; sells mobile devices and accessories; sells and rents fixed-line equipment; and offers network and platform services.

Market Cap: USD 40,630 million[3]
ENXTPA: ORA
Domicile: France
Website: www.orange.com

[1] For Orange's performance in the 2015 Index, see: https://rankingdigitalrights.org/index2015/companies/orange/.
[2] "Internal Security Code, Article L. 851-3" (2015).
[3] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 74%

Orange ranked second among telecommunications companies in the Governance category, after Vodafone, and received the third-highest score of all 22 companies.

Orange received the highest score among telecommunications companies for its disclosures about its human rights impact assessments (G4). The company, however, tied with Ooredoo for the second-lowest score on G6, which looks for clear disclosure by companies of a remedy and grievance mechanism allowing users to issue complaints about violations to their freedom of expression and privacy rights. In France, "data subjects" may bring privacy-related complaints to the French Data Protection Agency but Orange should provide users with information on that process as well as offer direct channels to users for grievance and remedy.

FREEDOM OF EXPRESSION 16%

Orange lagged behind Vodafone, Telefónica, and AT&T in the Freedom of Expression category, tying with América Móvil for the fourth-highest score of the 10 telecommunications companies evaluated.

Content and account restriction requests: Orange was one of six telecommunications companies to score no points on these indicators (F5-F7). It offered no information about how it handles or complies with government and other third party requests to restrict content or accounts.

Network management and shutdowns: Orange did not disclose if it engages in network management policies; only two other companies, Etisalat and Ooredoo, also received no credit on this indicator (F9). It also revealed little about its processes for responding to network shutdown requests, lagging behind Vodafone and Telefónica on this indicator (F10). The 2015 Intelligence Law authorizes French authorities to shut down service or restrict access to the internet, with the help of ISPs such as Orange. Orange should clearly disclose this obligation to its users.

Identity policy: Orange requires pre-paid customers to provide a government-issued ID to activate a SIM card, although there is no law in France explicitly requiring mobile operators to obtain this information from pre-paid subscribers (F11).

PRIVACY 26%

Orange ranked fourth among telecommunications companies in the Privacy category, behind Vodafone, AT&T and Telefónica.

Handling of user information: While Orange disclosed far less information about how it handles user information than Vodafone and AT&T, it performed better than most telecommunications companies on these indicators (P3-P8). It disclosed some information about what user information it collects (P3), shares (P4), and why (P5). Like all telecommunications companies other than AT&T, Orange disclosed no information about how long it retains this information (P6).

Requests for user information: Orange disclosed little about how it handles requests from governments and private parties for user information but received the third-highest score on these indicators after AT&T and Vodafone (P10, P11). While the company provided some data about government and private requests for user information, the company failed to provide data on such requests for many of the countries in which it operates, including France (P11).[4] When national law prohibits the release of such data, Orange should specify the legal barrier to disclosure.

Security: Orange disclosed less than most of its peers about its security policies, lagging behind AT&T, Telefónica, and Vodafone on these indicators (P13-P18). The company provided some disclosure of its systems to ensure the security of their products and services (P13), but had no information about what it does to address security vulnerabilities via a bug bounty program (P14). Like most companies evaluated, Orange had no disclosure of its processes for responding to data breaches (P15).

[4] "Orange Transparency Report on Freedom of Expression and Privacy Protection: Year 2015" (Orange), accessed February 25, 2017, https://www.orange.com/fr/content/download/37558/1150696/version/2/file/Transparency+report+on+freedom+of+speach+and+privacy.pdf.

TELEFÓNICA, S.A.

● Telecommunications Company

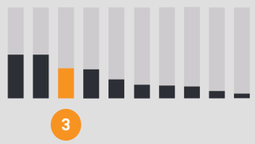
Key Findings:

- Telefónica's disclosure of its network shutdown policies was one of the more comprehensive among all telecommunications companies evaluated.
- The company had strong disclosure of its security policies, including measures it takes to safeguard users' information.
- The company offered insufficient disclosure about what user information it collects, shares, and retains, and how it handles requests from governments and private parties for user information.

OVERALL SCORE

33%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

TELEFÓNICA SPAIN

Spain

SERVICES EVALUATED

- Pre-Paid Mobile (Movistar)
- Post-Paid Mobile (Movistar)
- Fixed-Line Broadband (Movistar)

ANALYSIS

Telefónica ranked third out of the 10 telecommunications companies evaluated, behind AT&T and Vodafone, and 10th in the Index overall. Telefónica is new to the Index, making it the third European telecommunications company, along with Orange and Vodafone, evaluated by this Index. A member of the Telecommunications Industry Dialogue (TID), Telefónica made strong commitments to users' freedom of expression and privacy, although it fell 15 percentage points behind AT&T and Vodafone in its overall score. However, the company edged out Orange by one percentage point due to the company's comparatively stronger performance in the Freedom of Expression category. Nonetheless, the company had notably weaker disclosure of its commitments to freedom of expression and privacy at the governance level compared to its European peers. There appear to be few explicit legal factors in Spain, Telefónica's home market, that would prevent the company from making and disclosing stronger policies for implementing its commitments to users' freedom of expression and privacy or from disclosing much of the information relevant to this Index.

About Telefónica, S.A.

Telefónica, S.A. provides telecommunications services in Spain, Germany, the United Kingdom, and 14 countries in Latin America. It offers mobile and fixed line services, in addition to television, cloud computing, and other services. The company serves 274.8 million mobile phone, 38.9 million fixed telephony, over 21.7 million internet and data, and 8.3 million TV customers.[1]

Market Cap: USD 48,116 million[2]
BME: TEF
Domicile: Spain
Website: www.telefonica.com

[1] About Telefónica. **https://www.telefonica.com/en/web/about_telefonica/in_brief/key-figures**.
[2] S&P Capital IQ, Accessed February 13, 2017.

GOVERNANCE 58%

Telefónica ranked eighth out of all 22 in the Governance category. Among telecommunications companies, it fell behind Vodafone, Orange, and AT&T by a considerable margin.

Although Telefónica made a clear commitment to freedom of expression and privacy as human rights (G1), it was not clear whether there was senior-level oversight over these issues within the company (G2). The company also lacked disclosure of any human rights due diligence processes (G4). Notably, Telefónica received one of the higher scores for disclosing a grievance and remedy process through its online "responsible business channel," where users can submit questions and complaints about the company's policies and practices, including concerns regarding violations to freedom of expression and privacy.[3] But the company did not disclose how it responds to complaints or the number of complaints it receives.

FREEDOM OF EXPRESSION 27%

Telefónica placed third among the telecommunications companies in the Freedom of Expression category, behind Vodafone and AT&T but ahead of the rest of its peers.

Content and account restriction requests: Compared to AT&T and Vodafone, Telefónica disclosed little about how it handles government and private requests to restrict content and accounts, but it was one of only four telecommunications companies to receive any credit on these indicators (F5-F7). Telefónica's new transparency report, while a step in the right direction, did not provide adequate information about how it responds to these types of requests (F5),[4] or about the number of government requests it receives or complies with (F6)—although it was the only company other than AT&T to score any credit on this indicator. Like all telecommunications companies, Telefónica provided no data about private requests it may have received to remove content or accounts (F7).

Network management and shutdowns: Telefónica's lack of disclosure about its network management policies earned it one of the lowest scores of all telecommunications companies on this indicator (F9). However, it had the most comprehensive disclosure on network shutdowns, alongside Vodafone, although both companies still fell short of the standards required for full credit (F10).

Identity policy: Telefónica indicated it requires its pre-paid mobile users to provide identification (F11), in line with the legal requirements of Spain's data retention law.[5] As such Telefónica would be unable to change this policy without a change in the legal requirements.

PRIVACY 29%

Telefónica ranked third among telecommunications companies in the Privacy category, behind AT&T and Vodafone.

Handling of user information: Telefónica disclosed less than AT&T and Vodafone about how it handles user information, but scored on par with Orange and América Móvil on these indicators (P3-P8). While Telefónica disclosed some information on what user information it collects (P3), and for what purpose (P5), it provided no information about what user information it shares (P4). Like most telecommunications companies, apart from AT&T, the company did not reveal how long it retains user information (P6), or if and how users can obtain the information Telefónica holds on them (P8).

Requests for user information: Compared to AT&T and Vodafone, Telefónica provided little information about how it handles requests from governments and private parties for user information (P10-P11). Telefónica reported the number of requests to intercept communications and to obtain user metadata (P11), and the legal basis for them (P10). However, Telefónica lacked disclosure about its process for responding to requests, such as whether it commits to push back on overbroad requests.

Security: Telefónica had the second-highest score of all telecommunications companies on these indicators after AT&T (P13-P18). It received the highest score in the Index for disclosure of its processes for responding to data breaches (P15)—and was among only two other companies, AT&T and Vodafone, to receive any credit on this indicator.

[3] "Responsible Business Channel," **https://www.telefonica.com/en/web/about_telefonica/responsible-business-channel**.
[4] "Report on Transparency in Communications," (2016), **http://www.telecomindustrydialogue.org/wp-content/uploads/Telefonica_Transparencia_ENG_interactivo_29.12.pdf**.
[5] "Ley 25/2007, de 18 de Octubre, de Conservación de Datos Relativos a Las Comunicaciones Electrónicas Y a Las Redes Públicas de Comunicaciones."

VODAFONE GROUP PLC

● Telecommunications Company

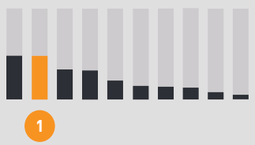
Key Findings:

- Vodafone tied with AT&T as the top-ranked telecommunications company in the 2017 Index.
- While it excelled in disclosures about network management and shutdowns, Vodafone had uneven disclosure about the circumstances and extent of content and account restrictions.
- Vodafone led the telecommunications companies in disclosures related to how user information is collected, shared, and otherwise handled, but could significantly improve its disclosure of how it secures user information.

OVERALL SCORE

48%

TELECOMMUNICATIONS RANK



OPERATING COMPANY EVALUATED

VODAFONE UK

United Kingdom

SERVICES EVALUATED

- Pre-Paid Mobile
- Post-Paid Mobile
- Fixed-Line Broadband

ANALYSIS

Vodafone tied with AT&T as the top-ranking telecommunications company of the 2017 Index, outpacing the third-ranked telecommunications company, Telefónica, by a 15-percentage point margin.[1] A member of the Telecommunications Industry Dialogue (TID), Vodafone made strong commitments to freedom of expression and privacy, but there is much room for improvement. At the corporate level, Vodafone made strong commitments to protect freedom of expression and privacy as human rights, but had notably weaker disclosure of its actual policies that affect users' freedom of expression and privacy in practice. The company should for instance produce evidence that it regularly conducts human rights impact assessments and should improve its transparency reporting by providing more detailed data on the government and private requests it receives to remove content or restrict accounts.

About Vodafone Group PLC

Vodafone Group Plc provides telecommunications services in Europe, Asia, Middle East, and Africa. The company serves 462 million mobile, 13.4 million fixed broadband, and 9.5 million TV customers.[2]

Market Cap: USD 65,290 million[3]
LSE: VOD
Domicile: United Kingdom
Website: www.vodafone.com

[1] For Vodafone's performance in the 2015 Index, see: **https://rankingdigitalrights.org/index2015/companies/vodafone**.
[2] "2016 Annual Report" (Vodafone, 2016), **http://www.vodafone.com/content/annualreport/annual_report16/downloads/vodafone-overview-2016.pdf**.
[3] S&P Capital IQ, accessed February 13, 2017.

GOVERNANCE 81%

Vodafone was the highest-scoring telecommunications company in the Governance category, topping AT&T by a wide margin, and receiving the second-best score of all 22 companies evaluated.

Vodafone publicly committed to respect freedom of expression and privacy as human rights (G1), and provided evidence of senior level oversight over these issues within the company (G2). However, Vodafone did not clearly disclose that it conducts regular human rights due diligence related to its products and services.[4] Vodafone tied with Bharti Airtel for the highest score on disclosure of its grievance and remedy mechanisms (G6); however, gaps remained in its disclosure. 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 receives or any evidence that it is responding to complaints.

FREEDOM OF EXPRESSION 45%

Vodafone was the highest-scoring telecommunications company in the Freedom of Expression category, outscoring AT&T by four percentage points and Telefónica by nearly 20.

Content and account restriction requests: Vodafone UK lagged behind AT&T for its disclosure of how it handles government and private requests to restrict content and accounts, but was one of only four telecommunications companies to receive any credit on these indicators (F5-F7). While the company had notably strong disclosure of its process for handling requests made by governments to remove or block content or restrict user accounts, it did not fully disclose how it handles such requests from other types of third parties (F5). It also disclosed no data about the number of requests it receives from governments or other third parties to restrict content or accounts (F6, F7).

Network management and shutdowns: Vodafone UK earned the highest score for its disclosure of its network management policies and was the only company to receive full credit for clearly committing not to block or prioritize content (F9). Like all telecommunications companies evaluated, it revealed little about its network shutdown policies, although it tied with Telefónica for the highest score on this indicator (F10).

Identity policy: Vodafone UK and AT&T were the only two telecommunications companies evaluated that did not disclose a requirement that users verify their identity with a government-issued ID for prepaid mobile services (F11).

PRIVACY 37%

In the Privacy category, Vodafone ranked second of 10 telecommunication companies, behind AT&T and ahead of Telefónica.

Handling of user information: Vodafone UK disclosed more than all other telecommunications companies about how it handles user information, including AT&T (P3-P8). However, it still did not sufficiently disclose what user information it collects (P3), shares (P4), and why (P5). It disclosed nothing about how long it retains user information (P6), like all telecommunications companies apart from AT&T. Notably, the company offered more information than any other telecommunications company about how users can access the information that Vodafone holds on them (P8).

Requests for user information: Vodafone UK disclosed less than AT&T about how it handles government and private requests for user information, but more than any other telecommunications company evaluated (P10, P11). Unlike AT&T, Vodafone did not disclose its process for responding to requests from private parties (P10).

Security: Vodafone UK disclosed less of its security policies than AT&T and Telefónica, the top-scoring telecommunications companies on these indicators (P13-P18). But it was one of only three companies in the entire Index to reveal any information about how it handles data breaches (P15), although its disclosure on this indicator was still significantly lacking in comparison to Telefónica, the top-scoring company on this indicator.

[4] "Sustainable Business Report 2015-16," **http://www.vodafone.com/content/dam/vodafone-images/sustainability/downloads/report2016.pdf**.

10. APPENDIX

10.1 Index Methodology Development

The Ranking Digital Rights Corporate Accountability Index was developed over three years of research, testing, consultation, and revision. Since inception the project has worked closely with researchers around the globe. For methodology development, pilot study, and the inaugural Index we also partnered with Sustainalytics, a leading provider of ESG (environmental, social, and governance) research to investors.

The first Corporate Accountability Index was launched in November 2015, applying the methodology to rank 16 internet and telecommunications companies.

For the 2017 Index, we expanded the ranking to cover additional types of companies and services, including those that produce software and devices that create what we call "mobile ecosystems." As a result, we also expanded the methodology, adding new indicators and elements to account for the potential threats to users' freedom of expression and privacy that can arise from use of networked devices and software. While we anticipate the need for small adjustments to the methodology as the project continues to develop and expand, our goal is to apply this same methodology in the 2018 edition of the Index in order to start producing year-on-year comparative data that will surface where companies are making improvements in their disclosure and where they are backsliding.

Research for the 2017 Index was conducted from September 1, 2016 through January 13, 2017. New information published by companies after that date was not evaluated.

To view or download the full 2017 methodology, visit: https://rankingdigitalrights.org/2017-indicators/.

For more information about the issues covered by the methodology, see pages 12 and 13.

Links to more detailed information about the project and its history can be found at the end of this Appendix.

10.2 Company Selection

The 2017 Index evaluates 10 telecommunications companies, 10 internet companies, and 3 companies that operate mobile ecosystems. One of the mobile ecosystems companies, Google, is also an internet company, bringing the total number of companies evaluated in the Index to 22.

For the full list of companies evaluated and how companies were grouped together for research and evaluation purposes, see page 11 and 12.

All companies evaluated in the Index are multinational corporations listed on a major stock exchange. The following factors influenced company selection:

- **User base:** The companies in the Index have a significant footprint in the areas where they operate. The telecommunications companies have a substantial user base in their home markets, and the internet companies have a large number of global users as identified by established global traffic rankings such as Alexa. The policies and practices of the selected companies, and their potential to improve, thus affects a large percentage of the world's 3.7 billion internet users.

- **Geographic reach and distribution:** The Index includes companies that are headquartered in North America, Europe, Africa, Asia, and the Middle East, and collectively, the companies in the Index have users in many regions around the world.

- **Relevance to users' freedom of expression and privacy rights:** Most of the companies in the Index operate in or have a significant user base in countries where human rights are not universally respected. This is based on relevant research from such organizations as Freedom House, the Web Foundation, and Reporters Without Borders as well as stakeholder feedback.

10.3 Selection of Services

The following factors guided the selection of services:

- **Telecommunications services:** These operators provide a breadth of services. To keep the scope of the Index manageable while still evaluating services that directly affect freedom of expression and privacy, the Index focused on: 1) post-paid and pre-paid mobile services, including the reasonable expected mobile offerings of voice, text, and data services; and, 2) fixed-line broadband, in cases where it was available in the company's home operating market. Only consumer services were included.

- **Internet services:** Two or three discrete services were selected based on their comparability across companies, the size of their user base, and their ability to paint a fuller picture of the overall company's approach to freedom of expression and privacy. This enabled researchers to discern whether company commitments, policies, and practices applied to the entire corporate entity or only to specific services.

- **Mobile ecosystems:** In 2016 most of the world's mobile devices were running either Apple's iOS operating system, or some version of Google's Android mobile operating system. Thus we evaluated Apple's iOS ecosystem plus two different variants of the Android ecosystem: Android on devices controlled directly by Google (the Nexus smartphone and Pixel tablet product lines), and Android on devices controlled by Samsung, which in 2016 held the largest worldwide market share for Android devices.

For a full list of company services evaluated in the Index, see pages 11 and 12.

10.4 Levels of Disclosure

The Index considered company disclosure on several levels—at the parent company level, the operating company level (for telecommunications companies), and the service level. This enabled the research team to develop as complete an understanding as possible about the level at which companies disclose or apply their policies.

For internet and mobile ecosystem companies, the parent company typically delivered the services. In some cases the service was also a subsidiary. However, the structure of these companies was

generally such that the subsidiary only delivered one service, which made it straightforward to understand the scope of policy disclosure.

For telecommunications companies, with the exception of AT&T, the parent company did not directly provide consumer services, so researchers also examined a subsidiary or operating company based in the home market to ensure the Index captured operational policies alongside corporate commitments. Given AT&T's external presentation of its group-level and U.S. operating company as an integrated unit, we evaluated the group-level policies for AT&T.

10.5 Research Process and Steps

RDR works with a network of international researchers to collect data on each company, and to evaluate company policies in the language of the company's operating market. RDR's external research team in 2017 consisted of 28 researchers from 19 countries. A list of our partners and contributors can be found at: https://rankingdigitalrights.org/who/affiliates/

The research process for the 2017 Index consisted of several steps involving rigorous cross-checking and internal and external review, as follows:

- **Step 1: Data collection.** A primary research team collected data for each company and provided a preliminary assessment of company performance across all indicators.
- **Step 2: Secondary review.** A second team of researchers conducted a fact-check of the assessment provided by primary researchers in Step 1.
- **Step 3: Review and reconciliation.** RDR research staff examined the results from Steps 1 and 2 and resolved any differences that arose.
- **Step 4: First horizontal review.** Research staff cross-checked the indicators to ensure they had been evaluated consistently for each company.
- **Step 5: Company feedback.** Initial results were sent to companies for comment and feedback. All feedback received from companies by the agreed upon deadline was reviewed by RDR staff who made decisions about score changes or adjustments.
- **Step 6: Second horizontal review.** Research staff conducted a second horizontal review, cross-checking the indicators for consistency and quality control.
- **Step 7: Final scoring.** The RDR team calculated final scores.

10.6 Company Engagement

Proactive and open stakeholder engagement has been a critical component of the Index's methodology. We communicated with companies throughout the research process.

Open dialogue and communication: Before the research began, we contacted all 22 companies and informed them that they were included in this year's Index, describing our research process and timeline. Following several stages of research and review, we shared each company's initial results with them. We invited companies to provide written feedback as well as additional source documents. In many cases, the research team conducted conference calls or meetings with companies that requested them to discuss the initial findings as well as broader questions about the Index and its methodology.

Incorporating company feedback into the Index: While engagement with the companies was critical to understand company positions and ensure the research reviewed relevant disclosure, the Index evaluates information that companies disclose publicly. Therefore we did not consider a score change unless companies identified publicly available documentation that supported a change. Absent that, the research team reviewed company feedback and considered it as context for potential inclusion in the narrative report, but did not use it for scoring purposes.

10.7 Scoring

The Index evaluates company disclosure of the overarching "parent," or "group," level as well as well as those of selected services and/or local operating companies (depending on company structure). Each indicator has a list of elements, and companies receive credit (full, partial, or no credit) for each element they fulfill. The evaluation includes an assessment of disclosure for every element of each indicator, based on one of the following possible answers:

- "Yes"/ full disclosure: Company disclosure meets the element requirement.
- "Partial" -- Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of the what the element is asking for.
- "No disclosure found" - Researchers were not able to find information provided by the company on their website that answers the element question.
- "No" - Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of "no disclosure found," although both result in no credit.
- "N/A" - Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company in the scoring process.

Points

- Yes/full disclosure = 100
- Partial = 50
- No = 0
- No disclosure found = 0
- N/A excluded from the score and averages

Companies receive a cumulative score of their performance across all Index categories, and results show how companies performed by each category and indicator. Scores for the Freedom of Expression and Privacy categories are calculated by averaging scores for each individual service. Scores for the Governance category indicators include group-, operating- and service(s)-level performance (depending on indicator and company type, see below).

Governance Category Scoring

- G1 and G5:
  - Internet and mobile ecosystem companies: scores were based on the "group" level scores;
  - Telecommunications companies: scores based on average "group" and operating company scores.
- G2, G3, G4:
  - Internet and mobile companies: scores based on average of "group"-level and services scores;
  - Telecommunications companies: Average of group, operating, and services scores

- G6:
  - Internet and mobile companies: Average of service-level scores.
  - Telecommunications companies: Average of service-level scores.

Indicator and Element Scoring

Telecommunications companies were evaluated on 32 of the 35 indicators; internet and mobile ecosystem companies were evaluated on 33 of the 35 indicators. Some elements within indicators were not applicable to certain services.

The following list identifies which indicators or elements were N/A for certain companies or services:

- F3, Element 2: N/A for search engines
- F3, Elements 4-5: N/A for pre-paid and post-paid mobile services
- F5-F7: N/A for e-mail services
- F6, Element 2: N/A for search engines
- F7, Element 2:N/A for search engines
- F8, Element 1: N/A for telecommunications companies
- F8, Elements 1 & 4: N/A for search engines
- F8, Elements 1-3: N/A for email services
- F9: N/A for internet companies and mobile ecosystems
- F10: N/A for internet companies and mobile ecosystems
- F11: N/A for post-paid mobile and fixed-line internet services; search engines
- P9: N/A for telecommunications companies
- P14, Elements 5, 6, 9: N/A for internet companies
- P16: N/A for telecommunications companies
- P16, Elements 3-4: N/A for internet services without private messaging functions
- P17: N/A for telecommunications companies; search engines

The following elements apply only to mobile ecosystems:

- P1, Element 4
- P2, Element 5
- P3, Elements 4-5
- P4, Elements 5-6
- P6, Elements 6-7
- P7, Element 5
- P8, Element 5
- P14, Elements 4, 7-8

10.8 Further Information

- For more information about RDR's methodology development, see: https://rankingdigitalrights.org/methodology-development/
- The 2015 Index can be viewed here: https://rankingdigitalrights.org/index2015/
- For more details about differences between the 2015 and 2017 methodology, see: https://rankingdigitalrights.org/2016/09/15/rdr-launches-2017-research/
- For more information about the project please see our "frequently asked questions": page: https://rankingdigitalrights.org/who/frequently-asked-questions/.

10.9 Charts and Tables

- 2017 Corporate Accountability Index Map
- 2017 Company Ranking
- Figure 1: 2017 Ranking
- Figure 2: Telecommunications Companies: Privacy Scores
- Figure 3: Governance Scores
- Figure 4: Disclosure of Grievance and Remedy Mechanisms (G6)
- Figure 5: Mobile ecosystems: Overall Scores
- Figure 6: Mobile ecosystems: Scores by Index category
- Figure 7: Disclosure of Government and Private Requests to Restric Content and Accounts (F5-F7)
- Figure 8: Data of Data on Terms of Service Enforcement (F4)
- Figure 9: Identity Policies (F11)
- Figure 10: Disclosure of Network Shutdown Policies (F10)
- Figure 11: Disclosure of Handling of User Information: Average Scores (P3-P9)
- Figure 12: Disclosure of Handling of User Information (P3-P9)
- Figure 13: Disclosure of Options for Users to Control Their Information (P7)
- Figure 14: Average Security Scores, by Indicator (P13-P18)
- Figure 15: Disclosure of Security Policies (P13-P18)
- Figure 16: Data Breaches (P15)
- Figure 17: Disclosure of Encryption Policies (P16)

Notes

1 “Guiding Principles on Business and Human Rights” (United Nations, 2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

2 “Principles,” Global Network Initiative, accessed February 27, 2017, https://globalnetworkinitiative.org/principles/index.php.

3 “Implementation Guidelines,” Global Network Initiative, accessed February 28, 2017, http://globalnetworkinitiative.org/implementationguidelines/index.php.

4 “Corporate Accountability Index,” Ranking Digital Rights, November 2015, https://rankingdigitalrights.org/index2015/.

5 Nathalie Maréchal, “What Do We Mean by Mobile Ecosystems?,” Ranking Digital Rights, September 15, 2016, https://rankingdigitalrights.org/2016/09/15/what-are-mobile-ecosystems/.

6 “RDR Launches 2017 Corporate Accountability Index Research Cycle,” Ranking Digital Rights, September 15, 2016, https://rankingdigitalrights.org/2016/09/15/rdr-launches-2017-research/.

7 For information about changes made to the methodology between 2015 and 2017 see: “2015 Corporate Accountability Index” (Ranking Digital Rights, November 2015), https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf and “Comparison of Indicators in the 2015 and 2017 Index Methodology” (Ranking Digital Rights), accessed February 28, 2017, https://rankingdigitalrights.org/wp-content/uploads/2016/09/RDRmethodologycomparisontable2017.pdf.

8 For the full set of indicators, definitions, and research guidance please visit: “2017 Indicators,” Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/.

9 “2017 Indicators: Governance,” Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#G.

10 “2017 Indicators: Freedom of Expression,” Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#F.

11 “2017 Indicators: Privacy,” Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#P

12 “Global Internet Report 2016” (Internet Society, 2016), https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.

13 Kenneth Olmstead and Aaron Smith, “Americans and Cybersecurity,” Pew Research Center: Internet, Science & Tech, January 26, 2017, http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

14 “End-User Perspectives on Digital Media Survey: Summary Report” (World Economic Forum, January 2017), http://www3.weforum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf.

15 “Global Commission on Internet Governance: One Internet” (Centre for International Governance Innovation and Chatham House, 2016), https://www.ourinternet.org/report.

16 Rebecca MacKinnon, Nathalie Maréchal, and Priya Kumar, “Corporate Accountability for a Free and Open Internet” (Centre for International Governance Innovation and Chatham House, December 2016), https://www.ourinternet.org/research/corporate-accountability-free-and-open-internet.

17 “Universal Declaration of Human Rights” (United Nations, December 10, 1948), http://www.un.org/en/universal-declaration-human-rights/.

18 “International Covenant on Civil and Political Rights” (United Nations, December 16, 1966), http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

19 “Guiding Principles on Business and Human Rights” (United Nations, 2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

20 “Transparency Reporting Index,” Access Now, accessed February 27, 2017, https://www.accessnow.org/transparency-reporting-index/.

21 “Case Study #3: Transparency Reporting,” New America, accessed February 27, 2017, https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/.

22 To read more about Index scoring, see “Evaluation and Scoring,” pages 11 and 12.

23 Due to methodology changes, company scores cannot be directly compared between the two Indexes (see About the Corporate Accountability Index, page 8). However we can and do note where company disclosure has improved or declined.

24 Global Network Initiative Principles, http://globalnetworkinitiative.org/principles/index.php; Telecommunications Industry Dialogue Principles, http://www.telecomindustrydialogue.org/wp-content/uploads/Telecoms_Industry_Dialogue_Principles_Version_1_-_ENGLISH.pdf.

25 “2017 Indicators: Governance,” Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#G.

26 “Public Report on the 2015/2016 Independent Company Assessments” (Global Network Initiative, July 2016), http://globalnetworkinitiative.org/sites/default/files/Public-Report-2015-16-Independent-Company-Assessments.pdf.

27 “Working Group 3: Privacy and Transparency” (Freedom Online Coalition, November 2015), https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf.

28 For several indicators in the Freedom of Expression category, the Index evaluated both user- and developer-facing terms of services agreements. For more on our assessment of mobile ecosystems, see: https://rankingdigitalrights.org/index2017/findings/mobileecosystems.

29 “2017 Indicators: F1. Access to terms of service,” Ranking Digital Rights, accessed March 1, 2017, https://rankingdigitalrights.org/2017-indicators/#F1.

30 “2017 Indicators: F4. Data about terms of service enforcement,” Ranking Digital Rights, accessed March 1, 2017, https://rankingdigitalrights.org/2017-indicators/#F4.

31 “2017 Indicators: F8. User notification about content and account restriction,” Ranking Digital Rights, accessed March 1, 2017, https://rankingdigitalrights.org/2017-indicators/#F8.

32 “Google Transparency Report - Government Requests to Remove Content,” Google, accessed March 1, 2017, https://www.google.com/transparencyreport/removals/government.

33 “2017 Indicators: P14. Addressing security vulnerabilities,” Ranking Digital Rights, accessed March 1, 2017, https://rankingdigitalrights.org/2017-indicators/#P14.

34 Arch Puddington and Bret Nelson, “Q & A: 10 Years of Decline in Global Freedom,” Freedom House: Freedom at Issue Blog, January 26, 2016, https://freedomhouse.org/blog/q-10-years-decline-global-freedom.

35 “Freedom on the Net 2016” (Freedom House, November 2016), https://freedomhouse.org/report/freedom-net/freedom-net-2016.

36 Philip Oltermann, “Germany to force Facebook, Google, and Twitter to act on hate speech,” The Guardian, 17 December 2016, https://www.theguardian.com/technology/2016/dec/17/german-officials-say-facebook-is-doing-too-little-to-stop-hate-speech; Chris Strohm and Sarah Frier, “Obama Seeks Silicon Valley to

Help in Fight Against Terrorism," Bloomberg, 6 January 2016, https://www.bloomberg.com/politics/articles/2016-01-08/u-s-seeking-tech-cooperation-to-counter-extremist-recruitment.

37 "2017 Indicators: Freedom of Expression," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#F.

38 "2017 Indicators: F4. Data about Terms of Service Enforcement," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#F4.

39 "Combating Violent Extremism," Twitter Blog, February 5, 2016, https://blog.twitter.com/2016/combating-violent-extremism.

40 "An Update on Our Efforts to Combat Violent Extremism," Twitter Blog, August 18, 2016, https://blog.twitter.com/2016/an-update-on-our-efforts-to-combat-violent-extremism.

41 "Content Removal Requests Report," Microsoft, accessed February 28, 2017, https://www.microsoft.com/about/csr/transparencyhub/crrr/.

42 Juniper Downs, "Why Flagging Matters," Official YouTube Blog, September 15, 2016, https://youtube.googleblog.com/2016/09/why-flagging-matters.html.

43 "A/HRC/29/32: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye" (United Nations Human Rights Council, May 22, 2015), http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32.

44 "The Mandatory Registration of Prepaid SIM Card Users" (GSMA, November 2013), http://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf.

45 "2017 Indicators: F11. Identity Policy," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#F11.

46 "Guidelines for Law Enforcement," Twitter Help Center, accessed February 23, 2017, https://help.twitter.com/articles/41949?lang=en.

47 United Nations Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet", Resolution A/HRC/32/L.20, 27 June 2016, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/L.20

48 According to research by Access Now, the number of documented network shutdowns was 56 in 2016, compared to 15 in 2015: "#KeepItOn," Access Now, accessed February 28, 2017, https://www.accessnow.org/keepiton/.

49 "Let's Keep The Internet On For Everyone," Internet Society, accessed February 28, 2017, https://www.internetsociety.org/lets-keep-internet-everyone.

50 "2017 Indicators: F10. Network Shutdown," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#F10.

51 "Privacy Policy," Twitter, September 30, 2016, https://twitter.com/privacy.

52 "2017 Indicators: P3. Collection of User Information," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#P3.

53 "2017 Indicators: P4. Sharing of User Information," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#P4.

54 "2017 Indicators: P6. Retention of User Information," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#P6.

55 David Shepardson, "FCC Chair to Block Stricter Broadband Data Privacy Rules," Reuters, February 24, 2017, http://www.reuters.com/article/us-usa-fcc-broadband-idUSKBN163222.

56 "2017 Indicators: P7. Users' Control over Their Own User Information," Ranking Digital Rights, accessed February 28, 2017, https://rankingdigitalrights.org/2017-indicators/#P7.

57 "Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout," Identity Theft Resource Center, January 19, 2017, http://www.idtheftcenter.org.

58 "2016 Global Internet Report: Executive Summary" (Internet Society, 2016), https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/09/2016-Global-Internet-Report-Exec-Summary.pdf.

59 "2017 Indicators: P15. Data breaches," Ranking Digital Rights, accessed February 27, 2017, https://rankingdigitalrights.org/2017-indicators/#P15.

60 "A/HRC/29/32: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye" (United Nations Human Rights Council, May 22, 2015), http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32.

61 See Riana Pfefferkorn, "The Burr-Feinstein Crypto Bill Would Gut Our Cybersecurity," The Center for Internet and Society, Stanford Law School, (April 26, 2016), http://cyberlaw.stanford.edu/publications/burr-feinstein-crypto-bill-would-gut-our-cybersecurity and Joe Uchill, "Report: New Feinstein-Burr encryption effort in works," The Hill, September 9, 2016, http://thehill.com/policy/cybersecurity/295236-report-new-feinstein-burr-encryption-effort-in-works.

62 Le Monde (2015), Lutte contre le terrorisme sur le Web: questions sur les mesures souhaitees par la police, http://www.lemonde.fr/pixels/article/2015/12/08/interdiction-de-tor-des-wi-fi-partages-les-mesures-souhaitees-par-la-police-en-question_4826828_4408996.html.

63 "Overview of the Package of Changes to a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism" (The International Center for Not-for-Profit Law, July 21, 2016), http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.

64 "2017 Indicators: P16. Encryption of user communication and private content," Ranking Digital Rights, accessed February 27, 2017, https://rankingdigitalrights.org/2017-indicators/#P16.

65 The New York Times, "Breaking Down Apple's iPhone Fight With the U.S. Government," The New York Times, March 3, 2016, https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html.

66 "Working Group 3: Privacy and Transparency" (Freedom Online Coalition, November 2015), https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf.

67 "Universal Declaration of Human Rights" (United Nations, December 10, 1948), http://www.un.org/en/universal-declaration-human-rights/.

68 "International Covenant on Civil and Political Rights" (United Nations, December 16, 1966), http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

69 "The International Principles on the Application of Human Rights to Communications Surveillance," Necessary and Proportionate, May 2014, https://necessaryandproportionate.org/principles.

70 "Manila Principles on Intermediary Liability," Manila Principles, accessed February 28, 2017, https://www.manilaprinciples.org/.

71 Global Commission on Internet Governance, "Securing Human Rights for Digital Citizens: Encryption and Anonymity," One Internet, (Centre for International Governance Innovation and The Royal Institute for International Affairs 2016), https://www.ourinternet.org/report#chapter-section--encryption-and-anonymity.