Ranking Digital Rights 2018

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

Table of contents

2018 Index Methodology

The 2018 Index measures company disclosure of policies and practices affecting users' freedom of expression and privacy. The Index methodology applies 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.[9]

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.[10]
- **Freedom of Expression (F)**: This category contains 11 indicators measuring company disclosure of policies that affect users' freedom of expression.[11]
- **Privacy (P)**: This category contains 18 indicators measuring company disclosure of policies and practices that affect users' privacy rights.[12]

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: This category includes both internet companies and companies that produce software and devices that we call "mobile ecosystems." These company types are evaluated together because Google is both an internet company and a mobile ecosystem company, and along with its iOS mobile ecosystem, Apple also offers services like iMessage and iCloud. In addition, the freedom of expression and privacy issues faced by mobile cloud data and operating systems overlap with the issues faced by traditional internet services. We do not evaluate hardware attributes of devices, focusing our assessment instead on their operating systems. Additional elements relevant only to mobile ecosystems were added to some indicators.

For each internet and mobile ecosystem 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
- **Google (U.S.)** — Search, Gmail, YouTube,Android mobile ecosystem
- **Kakao (South Korea)** — Daum Search, DaumMail, KakaoTalk
- **Mail.Ru (Russia)** — VKontakte, Mail.Ru email, Mail.Ru Agent
- **Microsoft (U.S.)** — Bing, Outlook.com, Skype
- **Oath (U.S.)** — Yahoo Mail, Flickr, Tumblr
- **Samsung (South Korea)** — Samsung implementation of Android
- **Tencent (China)** — QZone, QQ, WeChat
- **Twitter (U.S.)** — Twitter, Periscope

- **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 services, 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 (G1), 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 (G2), and employee training and whistleblower programs addressing these issues (G3); 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 (G4); systematic and credible stakeholder engagement, ideally including membership in a multi-stakeholder organization committed to human rights principles, including freedom of expression and privacy (G5); 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 (G6).

Terms of service and privacy policies: We expect companies to provide terms of service agreements and privacy policies that are easy to find and understand, available in the primary languages of the company's home market, and accessible to people who are not account holders or subscribers (F1, P1). We also expect companies to clearly disclose whether and how they directly notify users of changes to these policies (F2, P2).

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 (F3). 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 (F4), 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 (F8).

Handling user information: We expect companies to disclose what information they collect (P3), what information they share and the types and names of the third parties with whom they share it (P4), the purpose for collecting and sharing user information (P5), and for how long this information is retained (P6). Companies should also provide clear options for users to control what information is collected and shared, including for the purposes of targeted advertising (P7), and should clearly disclose if and how they track people across the web using cookies, widgets, or other tracking tools embedded on third-party websites (P9). We also expect companies to clearly disclose how users can obtain all public-facing and internal data they hold, including metadata (P8).

Handling of government and private requests: We expect companies to clearly disclose their process for responding to government and private requests to restrict content and user accounts (F5) and to hand over user information (P10). We expect companies to produce data about the types of requests they receive and the number of these requests with which they comply (F6, F7, P11). Companies should notify users when their information has been requested and disclose if laws or regulations prevent them from doing so (P12).

Identity policies: We expect companies to disclose whether they ask users to verify their identities using government-issued ID or other information tied to their offline identities (F11). 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 (F9). We also expect companies to clearly disclose their policies and practices for handling government network shutdown demands (F10). We expect companies to explain the circumstances under which they might take such action and to report on the requests they receive and with which they comply.

Security: We expect companies to clearly disclose internal measures they take to keep their products and services secure (P13), explain how they address security vulnerabilities when they are discovered (P14), and outline their policies for responding to data breaches (P15). We also expect companies to disclose that they encrypt user communications and private content (P16), that they enable features to help users keep their accounts secure (P17), and to publish materials educating users about how they can protect themselves from cybersecurity risks (P18).

1.4. Evaluation and scoring

Research for the 2018 Index ran from January 13, 2017 to January 12, 2018. New information published by companies after January 12, 2018 was not evaluated for this Index.

2017 Index score adjustments: Some company scores from 2017 were adjusted for comparison with the 2018 evaluation. Scores were adjusted at the element level, in accordance with clarified evaluation standards that were applied in the 2018 Index, or to include information not located during the 2017 Index cycle, or as a result of a re-assessment of the company's disclosure. These adjustments did not produce changes to any company position in the 2017 rankings or to any of the key findings highlighted in the 2017 Index. Each score adjustment, including a detailed explanation of the reason for each change, is recorded in each company's final dataset, which is publicly available for download at: https://rankingdigitalrights.org/index2018/download/.

Scoring: The Index evaluates company disclosure at the overarching "parent," or "group," level 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”.

Companies receive a cumulative score of their performance across all Index categories, and results show how companies performed in 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

(For more information on company selection, and evaluation and scoring, see the Appendix, in Chapter 11 of this report).

2. Introduction

The information and communication technology (ICT) sector faces a global crisis of confidence. As this report goes to press, Facebook is under fire for how user data was accessed and used by people whose goal was to manipulate democratic elections.[13] A major global travel website has had its systems broken into and customer data stolen.[14] A growing number of governments are shutting down internet access to entire regions for days on end to stop transmission of speech they do not like.[15] Blanket, pervasive surveillance in many countries makes it dangerous for activists and investigative journalists to work online.

The 2018 Edelman Trust Barometer, which surveys public trust in a range of institutions across the world, notes "a significant drop in trust in platforms, notably search engines and social media."[16] The internet has transformed billions of lives in so many positive ways in the span of a generation that internet access is now considered essential to economic opportunity, education, and political participation. Yet the Internet Society now warns that a decline of trust in networked technologies could deter some people from connecting at all, or cause them to engage with technologies much less than they would have otherwise.

Companies will not rebuild public trust without demonstrating—not just with words but with actions—that they are committed to protecting and respecting users' rights. Corporate profits must not come at the expense of human rights, whether the violations are committed directly by companies or whether companies indirectly facilitate human rights violations by governments as well as non-state actors ranging from Cambridge Analytica to the Islamic State.

If human rights are to be protected and respected around the world, the internet must be designed, operated, and governed in a way that reinforces the protection and exercise of human rights. That is not presently the case. The Ranking Digital Rights 2018 Corporate Accountability Index offers detailed evidence as to exactly *how* the world's most powerful internet, mobile, and telecommunications companies are failing to respect users' rights. Too few companies make users' rights a central priority for corporate oversight, governance, and risk assessment. Most withhold even basic information about measures they take to keep users' data secure. None disclose enough about how personal information is handled, including what is collected and shared, with whom, and under what circumstances. They are all much too opaque about how content and information flows are policed and shaped through their platforms and services.

But solutions require more than diagnosis. The Index thus offers a detailed and constructive roadmap for what companies can do to better respect users' freedom of expression and privacy. In so doing, we have created a clear framework for policymakers, investors, and civil society to use in helping, pushing—and even requiring when necessary—companies to build a better internet through which everyone can exercise their rights, and take full advantage of everything that the technology has to offer.

The Index results also highlight how government policy and regulation can either help or hinder the private sector's respect for users' freedom of expression and privacy. There is a clear lack of policy cohesion and coherence in and between many countries, making it more difficult for multinational companies to respect the rights of all users in a consistent manner. Other regimes actively violate international human rights standards; they demand private sector compliance with official censorship and surveillance efforts and often forbid companies from disclosing information about how they comply with such demands. Some jurisdictions make it impossible for companies to achieve high scores in the Index. Yet at the same time, we have identified specific ways that every single company can improve its policies and disclosures now, even in the absence of legal or regulatory change.

How to read this report: Chapters 3 - 7 focus on key findings from the 2018 Index data, highlighting areas of improvement since the 2017 Index was published as well as persistent concerns. While the Index evaluates companies across 35 different indicators, these five chapters focus on areas that we believe are of greatest concern and relevance—particularly in light of events of the past year. Chapter 4 focuses on security issues shared by all companies in the Index. Chapters 5 and 6 focus on privacy and expression issues specific to internet and mobile ecosystem companies. Chapter 7 focuses on issues specific to telecommunications companies. All of these chapters include recommendations for how companies can improve. Chapters 8 and 9 provide recommendations for how governments and investors can act upon the Index results. Chapter 10 contains individual "report cards" for all of the 22 companies evaluated in the Index, with specific findings and recommendations for each company. Chapters 1 and 11 provide important context and explanation for how research was conducted and how results were scored.

Find more details on the website: Despite its length, this report provides only highlights from the Index data. To view full comparative results of how every company scored on every indicator, and to see how different services within each company were evaluated, please explore the rest of the 2018 Index website.

The raw data can also be downloaded at: https://rankingdigitalrights.org/index2018/download/.

Beyond the Index: The 2018 Index covers 22 of the world's most powerful internet, mobile, and telecommunications companies. But that inevitably excludes companies and services that are important to people in specific countries and regions. Because our methodology and indicators are openly available, researchers in a range of countries and cities have begun to apply RDR's methodology to companies that are most relevant to them. We have compiled a list of the projects that have so far published their results on our website at: https://rankingdigitalrights.org/adaptations.

Beyond 2018: As technology and geopolitics evolve, we will continue to re-evaluate and adapt our methodology. In the second half of 2018, we hope to conduct research and consultations to determine what indicators may need to be added to address the need for corporate transparency around the deployment of algorithms and artificial intelligence, and how targeted advertising technologies affect users' rights. As always, we will report on progress and invite feedback on our website at: https://rankingdigitalrights.org.

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 on their public commitments and disclosed 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,[4] 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[5] and implementation guidelines,[6] 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 Index, which ranked 16 internet and telecommunications companies. For the 2017 Index, RDR expanded the ranking to 22 companies, which included all of the companies ranked in 2015 plus an additional six companies. In addition to internet and telecommunications companies, RDR added new types of services, including those that produce software and devices that we call "mobile ecosystems," and made further revisions to the methodology.[7] The 2018 Index applies the same methodology to evaluate the same 22 companies as in the 2017 Index.[8] This enabled us to produce comparative analyses of each company's performance and to track overall trends.

2018 CORPORATE
ACCOUNTABILITY
INDEX

Acknowledgments

Ranking Digital Rights (RDR) staff:

Rebecca MacKinnon, Director Amy Brouillette, Senior Research and Editorial Manager Lisa Gutermuth, Senior Program Manager Laura Reed, Senior Research Analyst and Coordinator Andrea Hackl, Research Analyst Ilana Ullman, Policy and Communications Analyst Afef Abrougui, Corporate Accountability Editor

We wish to thank Nat Meysenburg at Open Technology Institute for his input on the 2018 Index methodology. We also wish to acknowledge former Ranking Digital Rights team members for their work in developing the 2015 and 2017 Index methodologies: Priya Kumar, Research Analyst; Allon Bar, Policy and Engagement Manager; Nathalie Maréchal, Senior Research Fellow; Revati Prasad, PhD candidate, Annenberg School for Communication, University of Pennsylvania.

Contributing researchers

Shazeda Ahmed, Amanda Alemán Angelini, Opeyemi Akanbi, Riyadh Al-Balushi, Joan Barata, Alex Comninos, Luis Fernando García Muñoz, Elonnai Hickok, Sergei Hovyadinov, Kelly Kim, Shabina S. Khatri, Danielle Kehl, Priya Kumar, Tetyana Lokot, Carly Nyst, Gisela Pérez de Acha, Léa Richard, Tatevik Sargsyan, Mariam Al Shafie, Mingli Shi, Jiwon Son, Ann Spanger, Hu Yong, Joseph Yoo, Benjamin Zhou.

Design and layout: Alison Yost, Director of Strategic Communications and Outreach, New America's Open Technology Institute.

Graphics: Olivia Solis, SHARE Lab.

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

Special thanks: Matt Barg, Sustainalytics; Chris Ritzo, Senior Technologist at Open Technology Institute. Thanks also to Melissa Brown, Dipayan Ghosh, Priya Kumar, Bennett Freeman, Nathalie Maréchal, Carly Nyst, Tatevik Sargsyan, and Andi Wilson for providing valuable feedback about this report.

Funders The 2018 Corporate Accountability Index was supported by the following funders:

John D. and Catherine T. MacArthur Foundation • Ford Foundation • Open Society Foundations • U.S. Department of State, Bureau of Democracy, Human Rights, and Labor

For a full list of current and former project funders and partners, please see https://rankingdigitalrights.org/who/partners/.

About Ranking Digital Rights

Ranking Digital Rights is a non-profit research initiative housed at the New America Foundation’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 www.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.

11. Appendix

11.1 Index methodology development ## {#section-111}

The Ranking Digital Rights Corporate Accountability Index methodology was developed over three years of research, testing, consultation, and revision. Since its inception in 2013, the project has engaged 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, launched in March 2017, 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.

The 2018 Index applies the same methodology to evaluate the same 22 companies as in the 2017 Index.[108] This enabled us to produce comparative analyses of each company's performance and to track overall trends.

We encourage stakeholders to read more about our methodology development: https://rankingdigitalrights.org/methodology-development/

To view or download the full 2018 methodology, visit: https://rankingdigitalrights.org/2018-indicators/

11.2 Company selection ## {#section-112}

The 2018 Index evaluates 10 telecommunications companies and 12 internet and mobile ecosystem companies.

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 affect a large percentage of the world's 4.2 billion internet users.[109]

- **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.

11.3 Selection of services ## {#section-113}

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 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 Section 1.2.

11.4 Levels of disclosure ## {#section-114}

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.

11.5 Research process and steps ## {#section-115}

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 for the 2018 Index consisted of 28 researchers from or based in 18 countries. A list of our partners and contributors can be found at: https://rankingdigitalrights.org/who/affiliates/.

The research process for the 2018 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.

11.6 Company engagement ## {#section-116}

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. 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.

11.7 Evaluation and scoring ## {#section-117}

Research for the 2018 Index was based on company policies that were active between January 13, 2017 and January 12, 2018. New information published by companies after January 12, 2018 was not evaluated.

2017 Index score adjustments: Some company scores from 2017 were adjusted for comparison with the 2018 evaluation. Scores were adjusted at the element level, in accordance with clarified evaluation standards that were applied in the 2018 Index, or to include information not located during the 2017 Index cycle, or as a result of a re-assessment of the company's disclosure. These adjustments did not produce changes to any company position in the 2017 rankings or to any of the key findings highlighted in the 2017 Index. Each score adjustment, including a detailed explanation of the reason for each change, is recorded in each company's final dataset, which is publicly available for download here.

How companies are scored: The Index evaluates company disclosure of the overarching "parent," or "group," level, 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 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 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 ecosystem companies: scores based on average of “group”-level and services scores.

- Telecommunications companies: average of group, operating, and services scores.

- **G6:**

- Internet and mobile ecosystem 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, Cloud services, email services, and messaging services.

- F5-F7: N/A for email services

- F6, Element 2: N/A for search engines

- F7, Element 2: N/A for search engines

- F6, Element 3: N/A for messaging services

- 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 and mobile ecosystem companies

- F10: N/A for internet and mobile ecosystem companies

- 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 and Google and Apple mobile ecosystems

- P14, Elements 4, 7, 8: N/A for internet companies and telecommunications 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

11.8 For further information: ## {#section-118}

- 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/.

- The 2017 Index can be viewed here: https://rankingdigitalrights.org/index2017/.
- 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/.

11.9 Charts and tables ## {#section-119}

10. Company Report Cards

The 2018 Index ranks 22 internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting users' freedom of expression and privacy. For an analysis of each company's performance in the Index, read each company's individual report card in the COMPANIES section of the website.

3. Inadequate disclosure

While more than half of the companies evaluated in the past two Indexes have made meaningful improvements, they still fall short in disclosing basic information to users about the design, management, and governance of the digital platforms and services that affect human rights.

The Ranking Digital Rights Corporate Accountability Index measures the minimum disclosure standards that companies should meet in order to demonstrate respect for users' freedom of expression and privacy rights. Against the backdrop of geopolitical events of the past two years, the Index results highlight four areas of urgent concern:

1. **Governance: Too few companies make users' expression and privacy rights a central priority for corporate oversight, governance, and risk assessment.** Companies do not have adequate processes and mechanisms in place to identify and mitigate the full range of expression and privacy risks to users that may be caused not only by government censorship or surveillance, and by malicious non-state actors, but also by practices related to their own business models.
2. **Security: Companies lack transparency about what they do to protect users' information.** As a result, people do not know the security, privacy, and human rights risks they face when using a particular platform or service. As headlines of the past year have shown, security failures by companies have serious financial, political, and human rights consequences for people around the world.
3. **Privacy: Companies offer weak disclosure of how user information is handled: what is collected and shared, with whom, and under what circumstances.** Companies do not adequately disclose how user information is shared for targeted advertising. Such opacity makes it easier for digital platforms and services to be abused and manipulated by a range of state and non-state actors including those seeking to attack not only individual users but also institutions and communities.
4. **Expression: Companies keep the public in the dark about how content and information flows are policed and shaped through their platforms and services.** Despite revelations that the world's most powerful social media platforms have been used to spread disinformation and manipulate political outcomes in a range of countries, companies' efforts to police content lack accountability and transparency.

The average score for all 22 companies evaluated in the 2018 Index was just 34 percent. The highest score of any company was 63 percent. It is an understatement to say there is room for improvement: Even companies with higher scores have significant shortcomings in their policies and disclosures.

Research for the 2018 Index was based on company policies that were active between January 13, 2017 and January 12, 2018. New information published by companies after January 12, 2018 was not evaluated in this Index. Note that some of the 2017 Index scores cited in the 2018 Index were adjusted to align with the 2018 evaluation, please see Section 1.4 of this report for more information.

3.1 The 2018 Index ranking ## {#section-31}

![figure1](/assets/graphics/content/Figure 1. The 2018 Corporate Accountability Index ranking.png){:height="574px" width="949px" align="left"}

Google and Microsoft kept their lead among internet and mobile ecosystem companies, although the gap is narrowing. Google and Microsoft were the only companies in the entire Index to score more than 60 percent overall, but they made relatively few changes in the past year. These companies' leading positions are due to the fact that they disclose more information about more policies than all other companies in the Index. Neither company led the pack on every indicator, and both had particular areas in which their poor performance stood out. Microsoft's overall score actually declined slightly due to a reorganization of some of its information related to Skype (see Figure 2). Google underperformed on governance and ranked near the bottom on one indicator examining disclosure of what user information the company shares and with whom.

Facebook performed poorly on questions about the handling of user data. The company ranked fourth in the Index overall, raising its score by strengthening transparency reporting about lawful requests it receives to restrict content or hand over user data, and improving its explanation about how it enforces terms of service. However, while it ranked fourth in the Index overall, Facebook disclosed less about how it handles user information than six other internet and mobile ecosystem companies (Apple, Google, Kakao, Microsoft, Oath, and Twitter). Most notably, Facebook disclosed less information about options for users to control what is collected about them and how it is used than any other company in the Index, including Chinese and Russian companies (see Chapter 5).

Vodafone shot ahead of AT&T among telecommunications companies after making stronger efforts to demonstrate respect for users' rights. Vodafone is now the only telecommunications company in the Index to score above 50 percent. The company made meaningful improvements in several areas, notably on stakeholder engagement and due diligence mechanisms. It also improved its disclosure of how it responds to network shutdown demands, and how it handles data breaches. AT&T's score improvements were due primarily to new disclosure of how it responds to network shutdown orders from authorities, and improved disclosure of options users have to obtain their own data. Its governance score, however, dropped due to its decision not to join the Global Network Initiative (GNI) along with other former members of the now defunct Telecommunications Industry Dialogue.

See each company's individual "report card" in Chapter 10 of this report.

3.2 Notable changes ## {#section-32}

Most companies evaluated in the Index made progress over the last year: 17 of the 22 companies showed improvement.

Apple saw the greatest score increase among internet and mobile ecosystem companies, gaining eight percentage points in the 2018 Index. Much of this was due to improved transparency reporting. Apple also published information about policies and practices that were already known by industry insiders and experts but had not been disclosed on the official company website. Nonetheless, Apple still lagged behind most of its peers due to weak disclosure of corporate governance and accountability mechanisms, as well as poor disclosure of policies affecting freedom of expression.

![figure2](/assets/graphics/content/Figure 2. Year-on-year score changes (2017 to 2018).png "figure2")

Baidu and Tencent, the Chinese internet companies in the Index, both made meaningful improvements. Baidu made notable improvements to its disclosure of what user information it collects, shares, and retains. Tencent (which kept its substantial lead over Baidu) also made improvements to its disclosure of privacy, security, and terms of service policies. In the 2017 Index, we published an analysis of the Chinese company results and identified areas where these companies can improve even within their home country’s challenging regulatory and political environment.[18] The 2018 Index results showed that Chinese companies can and indeed do compete with one another to show respect for users’ rights in areas that do not involve government censorship and surveillance requirements.

For details on year-on-year changes for each company, see: https://rankingdigitalrights.org/index2018/compare.

Telefónica earned the biggest score change in the telecommunications category. The company increased its governance score by almost 20 percentage points by joining GNI and strengthening its corporate-level commitments, mechanisms, and processes for implementing those commitments across its business. Its overall score was further boosted by improvements to its transparency reporting on government and private requests to block content and for user information.

Many companies continued to improve their transparency reporting. In addition to Apple and Telefónica cited above, a number of other companies also made significant improvements in disclosing process information as well as data on government requests they received and complied with to restrict or block content, to shut down services, or to hand over user data. **Facebook** improved disclosure of its process for responding to third-party requests to restrict content or accounts, and it reported new data on private requests for the same. **Twitter** clarified which services its transparency reporting data applies to. **Oath** and **Orange** both improved disclosure of data about third-party requests for user information. All three European telecommunications companies—**Orange**, **Telefónica**, and **Vodafone**—plus **AT&T**, improved their disclosure of circumstances under which they comply with network shutdowns.

Despite these areas of progress, there is persistent lack of improvement in many areas. Chapters 4-7 focus on areas in which we have seen the least improvement: Chapter 4 examines the lack of transparency about security policies and practices; Chapter 5 highlights failure to disclose basic information about the collection, use, and sharing of user data by internet and mobile ecosystem companies; Chapter 6 examines continued opacity around the policing of content by internet platforms and mobile ecosystems; Chapter 7 analyzes the transparency shortfalls and challenges specific to telecommunications companies.

3.3 Governance advances and gaps ## {#section-33}

Companies are inconsistent and uneven in anticipating and mitigating risks and harms to users.

Strong governance and oversight are vital if companies are to anticipate and mitigate potential negative implications of their business and product decisions. Fortunately, many companies are actively working to improve in this area: this category of the Index saw the greatest overall score increase.

The Governance category of the Index evaluates whether companies demonstrate that they have processes and mechanisms in place to ensure that commitments to respect human rights, specifically freedom of expression and privacy, are made and implemented across their global business operations. In order to perform well in this section, a company's disclosed commitments and measures taken to implement those commitments should at least follow, and ideally surpass, the UN Guiding Principles on Business and Human Rights[19] and other industry-specific human rights standards focused on freedom of expression and privacy such as the Global Network Initiative Principles.[20] Specifically, measures should include board and corporate-level oversight, internal accountability mechanisms, risk assessment, and grievance mechanisms.

Companies with governance scores of higher than 70 percent were all members of the Global Network Initiative (GNI), a multistakeholder initiative focused on upholding principles of freedom of expression and privacy in relation to government requests. GNI member companies commit to a set of principles and Implementation Guidelines, which include due diligence processes as well as transparency and accountability mechanisms.[21] GNI also requires members to undergo an independent third-party assessment to verify whether they are implementing commitments in a satisfactory manner. The assessment results must then be approved by a multi-stakeholder governing board that includes human rights organizations, responsible investors, and academics, in addition to company representatives.

Companies with the most improved governance scores were **Telefónica**, **Orange**, and **Vodafone**, each of which joined GNI as full members in March 2017, and took measures to improve company commitments, oversight mechanisms, and due diligence in alignment with GNI implementation guidelines.

See Chapter 7 for a more detailed analysis of how telecommunications companies performed in the Index.

AT&T was the only non-GNI company with a governance score of more than 50 percent. However, the company's score in this category declined due to its weakened commitment to engaging with stakeholders on digital rights issues as a result of its decision not to join GNI along with its European peers and other members of the now-defunct Telecommunications Industry Dialogue.[22] While **Apple** and **Twitter** made meaningful improvements in the Governance category, their disclosed oversight and due diligence mechanisms were uneven, with many more gaps in their policies than GNI-member companies.

3.4 Spotlight: Human rights impact assessments ## {#section-34}

The greatest disparity in governance scores between GNI and non-GNI companies could be seen on Indicator G4. This indicator examines whether companies carry out regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of their business affect freedom of expression and privacy and to mitigate any risks posed by those impacts. There is a precipitous drop in disclosure from the top seven companies on this indicator, all GNI members who have made due diligence commitments, and Apple, the highest scoring non-GNI member with only 17 percent.

Human rights impact assessments (HRIAs) are a systematic approach to due diligence. A company carries out these assessments to determine how its products, services, and business practices affect the freedom of expression and privacy of its users. Such assessments should be carried out regularly. More targeted assessments should also be conducted to inform decisions related to new products, features, and entry into new markets.

While many companies in the Index that conduct HRIAs have shown some improvements over the past year, few conduct truly comprehensive due diligence on how all of their products, services, and business operations affect users' freedom of expression and privacy. Furthermore, companies that do conduct HRIAs mainly focus on privacy risk assessments and risks related to government censorship and surveillance demands. There is a notable lack of evidence (except from **Oath**) that companies conduct impact assessments on how their own terms of service rules and enforcement processes affect users' freedom of expression.

As discussed in Chapter 6, it is fair to expect companies to set rules prohibiting certain content or activities—like toxic speech or malicious behavior. However companies' commercial practices can have human rights implications that companies have a responsibility to understand and mitigate. For example, human rights activists have complained that thousands of videos uploaded to Google's YouTube by Syrian activists documenting alleged war crimes were removed removed because they violated rules against violent content.[23] In Myanmar, where access to Facebook via mobile phones is easier and less expensive than accessing other online websites and platforms, Rohingya activists fighting hate crimes and genocide have no alternative platform through which to reach their intended audience.[24] These companies should be conducting human rights impact assessments on how their terms of service enforcement mechanisms affect their users' ability to exercise and advocate for their rights. Yet neither Facebook nor Google provides any evidence that they in fact carry out such due diligence, though they do disclose that they conduct HRIAs in relation to government censorship and surveillance demands.

For more information about human rights impact assessments and links to a list of resources with practical guidance for companies, please visit: https://rankingdigitalrights.org/2018-indicators/#hria.

The 2018 Index did not look for disclosure about HRIAs on other aspects of companies' business models and product design, such as how user information is shared with advertisers and marketers, how targeted advertising is managed, how algorithms are used to organize and prioritize the display of content, or how artificial intelligence is deployed. When it becomes apparent that a process or technology has the potential to cause or facilitate violation of human rights, companies should be proactive in using HRIAs to identify and mitigate that harm. One laudable example not accounted for in the 2018 Index methodology is Microsoft's HRIA process on artificial intelligence technology, launched in 2017.[25] Adjustments to the Index methodology will be considered for future iterations so that companies which are proactive in anticipating and mitigating risks of emerging technologies will be appropriately rewarded, while failures to assess and mitigate known harms stemming from business processes and design choices may also be taken into account as appropriate.

3.5 Regulatory factors ## {#section-35}

Law, regulations, and political environments have a clear impact on companies' Index performance.

Governments compel companies to take actions for reasons of public order and national security that can sometimes clash with international human rights norms. Some governments also impose legal requirements, such as data protection laws, that bolster corporate protection and respect for users' rights when coherently implemented and enforced.

Companies evaluated in the Index operate across a global patchwork of regulatory and political regimes. Most national governments fall short, to varying degrees, of their duty to protect citizens' human rights. All companies in the Index face some legal or regulatory requirement in their home jurisdiction that prevents them from earning a perfect score on at least one indicator.

The companies at the bottom end of the Index face the greatest legal and regulatory obstacles in the jurisdictions where they are headquartered. In more restrictive or authoritarian regimes, one can find many legal barriers to disclosing the volume and nature of government requests to shut down networks, or to block or delete content. Yet laws that prevent clear public disclosure about the policing of online speech and denial of internet access can also be found in democracies and OECD countries, despite the fact that most such prohibitions are clearly inconsistent with basic principles of accountable governance. For example, in the UK, under limited circumstances, the law may prevent telecommunications operators from disclosing certain government requests to shut down a network.[26]

Meanwhile, legal interventions in Europe related to data protection and intermediary liability are expected to have significant impact on company respect for users' rights over the coming year.

Data protection: In May 2018, the European Union's General Data Protection Regulation ("GDPR") will come into force. For the purpose of the Ranking Digital Rights Corporate Accountability Index, the most significant impact of the GDPR on corporate business practices pertains to an expanded obligation of companies to disclose information to users.[27] Because research for this Index was completed in January 2018, as companies were still revising their policies and preparing for the GDPR, **the findings in this report should not in any way be seen as an evaluation of any company's GDPR compliance.** We expect that the 2019 Index will provide a clearer picture of the impact of the GDPR on company disclosure standards and best practices for handling of user information. However, since the RDR indicators do not fully overlap with the GDPR, future Index results can be taken as a measure of how the GDPR has improved company practices but not as a measure of legal compliance.

Outside of the EU, our legal analysis points to a strong relationship between Kakao's high scores on several indicators related to the handling of user information and South Korea's strong data protection regime, which requires companies to adhere to data minimization commitments and also contains strong disclosure requirements about collection, sharing, and use. Several jurisdictions where other Index companies are headquartered still lack adequate data protection laws, and companies headquartered in them tend to disclose no more than the law requires, leading to low privacy scores in the Index.

Increased liability for content: While European privacy regulations have generally been praised as a positive development for protecting internet users' rights, recent European efforts to hold internet platforms responsible for policing users' online speech have prompted criticism from human rights experts and advocates over concerns that such measures will lead to increased censorship of legitimate content.[28]

In May 2016, the European Commission announced a Code of Conduct on countering illegal online hate speech, signed by Facebook, Microsoft, Twitter, and YouTube (Google), each of which agreed to review requests to remove "illegal hate speech" within 24 hours, reviewing the content against their own terms of service as well as applicable national laws.[29] Germany's Network Enforcement Act (NetzDG), which came into full effect in January 2018, requires social media companies with more than 2 million registered users in Germany to develop procedures to review complaints and remove illegal speech. "Manifestly unlawful" content must be removed within 24 hours and most other "unlawful" content must be removed within seven days. Companies that fail to comply can be fined up to EUR 50 million.[30]

Civil society groups have criticized the Code of Conduct on countering illegal online hate speech for being overbroad and for incentivizing companies to remove content when in doubt about its legality, thus over-censoring content and making violations of users' free speech rights inevitable.[31] Germany's NetzDG law has also come under fire for giving private companies excessively broad power to adjudicate speech without sufficient judicial oversight or remedy. Human rights groups have also pointed to troubling efforts by other governments to duplicate such measures in jurisdictions where religious, political, and other speech that is protected under international human rights law is deemed "illegal" by domestic legislation.[32]

Against the backdrop of these trends, the 2018 Index results highlight a persistent and widespread lack of transparency by companies around the policing of content—especially about their terms of service enforcement. Indeed, we found that companies that signed on to the Code of Conduct on countering illegal online hate speech have not disclosed sufficient information about what content they have restricted in compliance with the code or any other information about how their compliance processes work.[33] (See Chapter 6 for detailed analysis of these findings.)

Without a strong commitment by companies to be more transparent about how they handle requests by governments and other third parties to restrict content, and about how they enforce their own rules, it will be all the more difficult for users to seek redress when their expression rights are violated in the course of corporate attempts to comply with new regulations and codes of conduct.

Furthermore, in order for users to obtain remedy when their expression rights are violated, they need accessible and effective mechanisms to do so. The 2018 Index found no other substantive improvements in the disclosed grievance and remedy mechanisms by internet and mobile ecosystem companies, despite a steady stream of media reports of activists and journalists being censored on social media.[34]

3.6 Recommendations for companies ## {#section-36}

The individual company report cards pinpoint how jurisdictional factors affect each company's scores in specific ways. Despite seriously flawed regulatory regimes across the world, Index results pinpoint many specific ways that all companies can improve even with no changes to their legal and regulatory environments.

Do not wait for the law to improve. Do everything possible now to maximize respect for users' rights. Companies should not wait for laws to be passed that require them to improve their privacy policies, publish transparency reports, improve governance, or carry out due diligence to mitigate risks. All companies in the Index can improve their scores substantially simply by improving policies in accordance with best practice standards articulated in each indicator, to the greatest extent legally possible. Unfortunately, many companies fail to disclose basic information and data that will help users understand the circumstances under which content or access is restricted or who can obtain their personal data, even when the law does not forbid disclosure of much of this information.

Disclose evidence that the company has institutionalized its commitments. It is certainly important for a company's top executives to express their personal commitment to respect users' rights. However, such commitments must be clearly institutionalized to ensure that policies are not being applied inconsistently, or do not depend on the tenure of specific individuals. There should be oversight at the board and executive level over how the company's business operations affect privacy and freedom of expression. This oversight must be accompanied by other measures such as company-wide training and internal whistleblowing mechanisms.

Conduct regular impact assessments to determine how the company's products, services, and business operations affect users' 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, and to enhance users' enjoyment of those rights. While it may be counterproductive for companies to publish all details of their processes and findings in all circumstances, it is important to disclose information showing 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 2018, only the Global Network Initiative meets the requirements for such an accrediting organization.

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.

Clarify for users what types of requests the company will—and will not—consider, and from what types of parties. For example, some companies make clear that they will only accept government requests for user information or to restrict content 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 and under what circumstances. Without clear policy disclosure about the types of requests the company is willing to entertain, users lack sufficient information about risks that they are taking when using a service.

Commit to push back against excessively broad or extra-legal requests. Companies should make clear that they will challenge requests that fail to meet requirements of lawful requests, including in a court of law.

Publish comprehensive transparency reports. Companies should publish regular information and data on their official websites that helps users and other stakeholders understand the circumstances under which personal information may be accessed, speech may be censored or restricted, or access to service may be blocked or restricted. Such disclosures should include 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.[35]

Work with other stakeholders including civil society, academics, and allies in government to reform laws and regulations in ways that maximize companies' ability to be transparent and accountable to users. The sector will benefit—and so will society as a whole—if public trust in ICT companies can be earned through broad commitment and adherence to best practices in transparency and accountability.

Invest in the development of new technologies and business models that strengthen human rights. Collaborate and innovate together with governments and civil society. Invest in the development of technologies and business models that maximize individual control and ownership over personal data and the content that people create.

Executive summary

The Ranking Digital Rights 2018 Corporate Accountability Index evaluated 22 of the world's most powerful internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy. These companies held a combined market capitalization of approximately USD 4.7 trillion.[1] Their products and services are used by a majority of the world's 4.2 billion internet users.[2] There is good news and bad news:

The good news: **More than half of the companies evaluated in the 2018 Index improved disclosure in multiple areas affecting users' freedom of expression and privacy.** In all, 17 of the 22 companies improved scores on at least one indicator. Even companies headquartered in the world's toughest regulatory environments are making efforts to improve. Positive trends included:

- **Transparency reporting continues to improve and expand.** More companies disclosed more information and data related to their policies and processes for responding to government or other third party requests to restrict content, as well as to share user information with authorities.

- **Telecommunications companies that joined the Global Network Initiative (GNI) pulled ahead of others in the sector.** In 2017, three European telecommunications companies evaluated by the Index (Orange, Telefónica, and Vodafone) joined GNI, a multi-stakeholder initiative that works with companies to advance human rights principles in the face of government censorship and surveillance demands. All three strengthened disclosure about governance, oversight, due diligence, and internal accountability mechanisms.

The bad news: **Companies are not transparent enough about the design, management, and governance of digital platforms and services that affect human rights.** If people lack the information necessary to understand how state and non-state actors exert power through digital platforms and services, it is impossible not only to protect human rights—but to sustain open and democratic societies. Transparency is essential in order for people to even know when users' freedom of expression or privacy rights are violated either directly by—or indirectly through—companies' platforms and services, let alone identify who should be held responsible. There are four areas of particularly urgent concern:

- **Governance: Too few companies make users' expression and privacy rights a central priority for corporate oversight and risk assessment.** Companies do not have adequate processes and mechanisms in place to identify and mitigate the full range of expression and privacy risks to users that may be caused not only by government censorship or surveillance, and by malicious non-state actors, but also by practices related to their own business models.

- **Security: Most companies withhold basic information about measures they take to keep users' data secure,** leaving users in the dark about risks they face when using a particular platform or service. At the same time, security failures by companies have serious economic, financial, political, and human rights consequences for people around the world.

- **Privacy: Companies don't disclose enough about how users' information is handled, including what is collected and shared, with whom, and under what circumstances.** This includes how user information is shared for targeted advertising. Such opacity makes it easier for digital platforms and services to be abused and manipulated by a range of state and non-state actors, including those seeking to attack institutions and communities, as well as individual users.

- **Expression: Companies do not adequately inform the public about how content and information flows are policed and shaped** through their platforms and services. In light of revelations that the world's most powerful social media platforms have been used to spread disinformation and manipulate political outcomes in a range of countries, companies' efforts to police and manage content lack accountability without greater transparency.

The 2018 Index evaluated companies on 35 indicators examining disclosed commitments and policies affecting freedom of expression and privacy, including corporate governance and accountability mechanisms.

Company highlights

- For the second year in a row, **Google** and **Microsoft** remain the only companies in the entire Index to score more than 60 percent overall. However both made relatively few changes in the past year. Their leading positions are due to the fact that they disclosed more information about more policies than other companies in the Index. Neither company led the pack on every indicator and each had areas of poor performance compared to other internet and mobile ecosystem companies in the Index.

- **Vodafone** shot ahead of **AT&T** and is the only telecommunications company in the Index to score more than 50 percent. Vodafone made meaningful improvements to disclosure about governance and due diligence processes, disclosed more information about how it responds to network shutdown demands, and was the only company in the Index to clearly inform users and the public about how it handles data breaches.

- **Facebook** performed poorly on questions about safeguarding user data. The company ranked fourth in the Index overall, raising its score by strengthening transparency reporting about lawful requests it receives to restrict content or hand over user data, and improving its explanation about how it enforces terms of service. However, Facebook disclosed less about how it handles user information than six other internet and mobile ecosystem companies. Most notably, Facebook disclosed less information about options for users to control what is collected about them, and how it is used, than any other company in the Index, including Chinese and Russian companies.

- **Apple** saw the greatest score increase, gaining eight percentage points. Much of this improvement was due to improved transparency reporting, plus new direct disclosure to users on its own website of information that it had previously only disclosed to experts and other third parties.

- Chinese internet companies **Baidu** and **Tencent** made meaningful improvements on disclosure of handling of user information and terms of service enforcement. While China's legal environment handicaps Chinese companies in the Index, these results nonetheless show that Chinese companies can—and do—compete with one another to improve transparency in areas that are not directly related to compliance with government censorship and surveillance requirements.

Recommendations

If the internet is to be designed, operated, and governed in a way that protects and respects human rights, we must all play our part. Companies, governments, investors, civil society organizations, and individuals—as employees of companies, as citizens of nations, as consumers of products, and as users of a globally interconnected internet—must all take responsibility and act.

Corporate transparency and accountability is incomplete without transparent and accountable governments that fulfill their duty to protect human rights. Meanwhile, companies should be held responsible for all the ways that their products, services, and business operations affect users' rights, over which they have any influence or control.[3] All companies evaluated in the Index can make many changes immediately, even in the absence of legal and policy reform. Detailed recommendations are listed throughout the Index report and in the individual company report cards. They fall under seven broad categories:

1. **Strengthen corporate governance:** Companies should not only articulate clear commitments to respect users' freedom of expression and privacy, but also disclose concrete evidence that they have institutionalized these commitments through board and executive oversight, company-wide training, internal reporting, and whistleblowing programs.

2. **Get serious about risk assessment:** Companies should implement comprehensive due diligence processes to ensure they can anticipate and mitigate any negative impact that their products, services, and business operations may have on users' rights.

3. **Provide meaningful grievance and remedy mechanisms:** Companies should have channels for users and other affected parties to file grievances if their rights have been violated as a result of company actions. Companies should also have clearly disclosed processes for responding to complaints and providing appropriate redress.

4. **Be transparent and accountable:** Companies should publish regular information and data on their official websites that helps users and other stakeholders understand the circumstances under which personal information is accessed by third parties, speech is censored or restricted, and access to a service is blocked or restricted.

5. **Strengthen privacy:** Companies should clearly inform users about what happens to their information, minimize collection and use of data to what is necessary for provision and service, and provide users with maximum control over what information they provide and with whom it is shared.

6. **Strengthen security:** Companies should disclose credible evidence of their efforts to secure users’ information. Specifically, they should show that they maintain industry standards of strong encryption and security, conduct security audits, monitor employee access to information, and have an established process for handling data breaches.

7. **Innovate for human rights:** Collaborate with government and civil society. Invest in the development of new technologies and business models that strengthen human rights, and maximize individual control and ownership over personal data and content.

6. Policing speech

Users are in the dark about the role that governments, private parties, and companies themselves play in policing the flow of information online.

Internet and mobile ecosystem companies act as powerful gatekeepers of global communication flows. Companies police content and regulate access to services according to their own private rules, and also at the request of governments and other third parties.

It is fair to expect companies to set rules prohibiting certain content or activities—like toxic speech or malicious behavior. However, when companies develop and enforce rules about what people can do and say on the internet—or whether they can access a service at all—they must do so in a way that is transparent and accountable. It is also fair to expect governments to set limits on freedom of expression for these companies to abide by, so long as those limitations are lawful, proportionate, and for a justifiable purpose, as outlined in international human rights instruments.[60] But people have a right to know how and why their speech or access to information may be restricted or otherwise shaped by companies—whether at the behest of governments, in compliance with laws, or for the companies' own commercial reasons.

The 2018 Index therefore includes six indicators measuring corporate transparency about processes for censoring online content or restricting access to their platforms or services. Collectively, these indicators evaluate company disclosure of policies and mechanisms for compliance with government requests, court orders, and other lawful third-party requests as well as for the enforcement of private rules, set by the company, about what types of speech and activities are permissible.[61] We expect companies to clearly disclose what types of content and activities they prohibit (F3), and to publish data about the volume and nature of content and accounts they remove or restrict for violating these rules (F4). Companies should also clearly disclose policies for responding to all types of third-party requests to restrict content and user accounts (F5), and publish data about the types of such requests they receive and with which they comply (F6, F7). We expect companies to notify users when they have removed content, restricted a user's account, or otherwise restricted access to content or a service (F8).

6.1. Transparency and accountability ## {#section-61}

Despite some positive steps, internet and mobile ecosystem companies still don't disclose enough about their role in policing online speech.

While companies continued to make steady improvements to transparency reporting, particularly about government requests, there is still much room for improvement. Results of the 2018 Index show limited overall improvement in the past year by internet and mobile ecosystem companies in publicly disclosing data and other information about all the ways that content is policed and managed on their platforms (Figure 14).[62]

As Figure 14 illustrates, most companies disclosed something about what content or activities are prohibited (F3), while few revealed anything about actions they take to enforce these rules (F4). Two companies—**Facebook** and **Tencent**—improved their disclosure of terms of service enforcement (F3), but companies across the board failed to provide enough information about these practices for users to understand what actions companies take to enforce their terms of service or how these actions affect users (see Section 6.2).

Five companies—**Apple, Facebook, Telefónica, Twitter,** and **Oath**—improved their disclosure of how they handle government requests to censor content and restrict accounts, but all lacked key information about how they respond to such demands. (see Section 6.3).

For companies to be fully transparent with users about their role in policing content or restricting access, they must notify users in the event of content or account restrictions. They must also provide information to those who are attempting to access content that has been removed, and clearly disclose the reason why. As Figure 14 shows, companies overall lacked clear commitments to notify users when and why they remove content, with an average score of just 22 percent among internet and mobile ecosystem companies on this indicator. Three companies—**Facebook, Oath**, and **Twitter**—improved their disclosure of policies for notifying users when accessing content that has been removed (F8). However, **Microsoft** lost points on this indicator for removing information that was previously available about policies for notifying Skype users when their accounts have been suspended.

6.2. Terms of service enforcement ## {#section-62}

Internet and mobile ecosystem companies lack transparency about what their rules are and actions they take to enforce them.

Internet and mobile ecosystem companies have come under growing pressure from policymakers and the public to better police the content that appears on their platforms due to concerns about hate speech, harassment, violent extremism, and disinformation. At the same time, companies must be transparent and accountable for how they set rules about what is allowed on their platforms and how decisions are made to enforce them. The Index contains two indicators evaluating how transparent companies are about what their rules are and how they are enforced. We expect companies to clearly disclose what types of content and activities they prohibit on their services and the process for enforcing these rules (F3). We also expect companies to publish data about the volume and nature of content and accounts they have removed or restricted for violating their terms (F4).

Results of the 2018 Index show that while internet and mobile ecosystem companies disclosed at least some information about what types of content or activities are prohibited by their terms of service, most disclosed nothing about the actions they took to enforce these rules (Figure 15).

- **Facebook** disclosed more than the rest of its peers about what content and activities it prohibits and its processes for enforcing these rules (F3). The company improved its disclosure of methods it uses to identify prohibited content, including user-flagging mechanisms, studying activity patterns, the use of artificial intelligence, and partnerships within industry and with civil society and governments.[63] These improvements since the 2017 Index put the company ahead of Microsoft and Kakao, which previously received the highest scores on F3.

- **Kakao** and **Microsoft** disclosed more information than most other internet and mobile ecosystem companies, apart from Facebook. Disclosures included some information about their processes used to identify prohibited content or accounts. Both companies provided clear information about what content they prohibit and why they might restrict a user's account, as well as some information about the processes they use to identify offending content or accounts and their process for enforcing their rules.

- **YouTube (Google)** and **Facebook** were the only social media platforms to receive full credit for their disclosure of mechanisms and processes used to identify prohibited content or activities. YouTube, like Facebook, disclosed information about a range of different types of tools it uses, including a community guidelines flagging process, staff reviews, and a system to help users identify copyrighted content.[64]

- **Tencent** improved its disclosure by providing more examples to illustrate how it enforces its rules (F3). This shows that companies operating in more restrictive environments can improve in this area without regulatory change.

- **Just four companies—Facebook, Google, Microsoft, and Twitter—disclosed any data about the volume or type of content or the number of accounts they restrict for violating their rules, and even these companies fell short.**

Companies should not only be transparent about what the rules are but they should also reveal what actions they take to enforce them. We expect companies to clearly disclose data on the volume and nature of content or accounts they restricted for terms of service violations, including the reasons for doing so. This means reporting data on the amount of content removed for containing hate speech, pornography, or extremist content—so long as these types of content are specifically and clearly prohibited in the terms of service—as well as disclosing the number of accounts suspended and why.

Index data shows that companies are making incremental progress in this area: in the 2015 Index, no company disclosed any data about the volume or nature of content or accounts restricted for violating their rules. In the 2017 Index, three companies—**Google, Microsoft**, and **Twitter**—each received a small amount of credit for disclosing some data about content they removed for terms of service violations, although all still failed to provide comprehensive or systematic data on these actions.[66] In the 2018 Index, four companies—the same three companies that received credit in the 2017 Index plus **Facebook**—divulged some information about different actions they took to enforce their terms of service. But a closer look reveals serious gaps in disclosure:

- **Twitter**: Twitter stated in a blog post that it suspended 235,000 accounts for violating its policies related to promotion of terrorism over a six-month span in 2016, but the company did not report information beyond this time period.[67] It also reported the number of times it removed content based on requests from government officials who flagged content that violated the terms of service.[68]

- **Microsoft**: Microsoft published data about its removal of “non-consensual pornography” in breach of its terms of service, but did not report any other data about actions it took to enforce other types of terms of service violations.[69]

- **Google**: Google gave some data on content removals from YouTube, although the data was not comprehensive or consistent. In September 2016, YouTube stated that in 2015 the company removed 92 million videos for violating its terms of service.[70] It also reported that one percent of the videos it removed were for hate speech and terrorist content.

- **Facebook**: The company in 2017 stated that in an effort to combat the spread of misinformation, it identified and removed more than 30,000 fake accounts in France. But it did not report information about removals from any other countries or the scope of these removals in general.[71] Facebook also reported that during the months of April and May 2017, it had removed around 288,000 posts each month, globally, for containing hate speech, but it does not report this information systematically.[72]

Most internet and mobile ecosystem companies failed to disclose how they identify content or activities that violate their rules—and none revealed if they give priority to governments or other third parties to flag content or accounts that breach these rules.

While all of the internet and mobile ecosystem companies in the 2018 Index disclosed at least some information about what types of content or activities they prohibit and reasons why they might restrict a user's account, fewer disclosed clear information about what processes they use to identify offenses on their platforms. Users have a right to know whether their content might be taken down through automated processes, human reviewers, or some combination of these and other methods. Users also have a right to know whether the platforms they use give priority consideration to "flagging" by governments or private individuals.

Some companies are known to designate specific individuals or organizations for priority consideration when they report or "flag" content that violates their terms of service.[73] YouTube is credited in the 2018 Index for disclosing information about its "trusted flaggers" program, in which more robust tools are provided to "people or organizations who are particularly interested in and effective at notifying us of content that violates our Community Guidelines."[74] This program is credited in media reports with helping reduce extremist content on the platform.[75] In 2016, the European Commission announced an agreement with Facebook, Microsoft, Twitter, and YouTube (Google) to remove hate speech online, and which encourages companies to "strengthen their ongoing partnerships with civil society organisations who will help flag content."[76] In 2017, Indonesian media reported that YouTube and Twitter would allow "selected users to flag material deemed as being linked to terrorism."[77]

However, companies do not disclose much information about how these systems work in practice. While YouTube disclosed information about priority flagging processes for private parties (F3, Element 5), no company disclosed if they give priority flagging status to individuals employed by governments (F3, Element 4). Nor is it clear how or whether a company assesses the independence or motivations of a private flagger.

What is priority flagging? Companies that host public or user-generated content may have systems in place to allow users to "flag" content or accounts that they think violates the company's rules. Once an item is flagged, some person (or system) at the company must decide whether to take action and if so, whether to remove or restrict access to the content, whether to take action against the user who posted it, or whether to take no action at all (for example, if the content was flagged erroneously). We expect companies to disclose information about the processes they use to identify content or activities that violate their rules, including if they use flagging mechanisms. In addition, if content or accounts flagged for violating a company’s rules by a government official or a particular person or group is given extra consideration, immediate review, or prioritization through other means, we expect companies to clearly disclose this information.

Users of internet and mobile platforms have a right to know if authorities from their own government (or any other government that they may want to criticize publicly) are availing themselves of such priority status, thereby enabling them to circumvent the process of serving the company with an official government request or court order, which would be included in company transparency reports and become a matter of public record in many countries. Information about the volume and nature of content being censored at the behest of government authorities—whether formally or informally—is essential for users to identify abuse of a platform’s content policing system. Without such information it is not possible to hold companies or authorities fully and appropriately accountable when users’ expression rights are violated. Yet companies keep us largely in the dark about whether governments are availing themselves, directly or indirectly, of informal flagging mechanisms.

6.3. External requests to restrict content and accounts ## {#section-63}

Companies lack transparency about how they handle formal government and private requests to censor content or restrict accounts.

Aside from platforms’ private mechanisms for flagging terms of service violations, internet and mobile ecosystem companies receive a growing number of external requests to remove content or restrict user accounts via more formal and official channels. These requests come from government agencies, law enforcement, and courts, who ask companies to remove content that violates the law, infringes on someone’s privacy, or contains hate speech, extremist content, or pornography. Requests can also come from self-regulatory bodies, like the UK’s Internet Watch Foundation [78], or from individuals who can ask companies to remove content under the 2014 “Right to be Forgotten” ruling,[79] or through a notice-and-takedown system such as the U.S. Digital Millennium Copyright Act.[80]

How does RDR define government and private requests? Government requests are defined differently by different companies and legal experts in different countries. For the purposes of the Index methodology, all requests from government ministries or agencies, law enforcement, and court orders in criminal and civil cases, are evaluated as “government requests.” Government requests can include requests to remove or restrict content that violates local laws, restrict users’ accounts, or to block access to entire websites or platforms. We expect companies to disclose their process for responding to these types of requests (F5), as well as data on the number and types of such requests they receive and with which they comply (F6). **Private requests** are considered, for the purposes of the Index methodology, to be requests made by any person or entity through processes that are not under direct governmental or court authority. Private requests can come from a self-regulatory body such as the Internet Watch Foundation, through agreements such as the EU's Code of Conduct on countering hate speech online, from individuals requesting to remove or de-list content under the "Right to be Forgotten" ruling, or through a notice-and-takedown system such as the U.S. Digital Millennium Copyright Act (DMCA). **See Index glossary of terms at:** https://rankingdigitalrights.org/2018-indicators/#Glossary

Although a handful of companies made notable improvements to their transparency reporting, as Figure 16 illustrates most companies in the 2018 Index failed to disclose sufficient information about how they handle government and private requests to censor content and restrict user access (see Section 6.1).

In general, and as was also the case in the 2017 Index, most companies tended to do better at disclosing about their processes for responding to government or private requests to remove content or restrict accounts (F5), than they did at reporting actual data about the number and type of government and private requests they received and with which they complied (F6, F7).

Notably, **Google** and **Facebook** earned the highest marks for disclosing their processes for responding to third-party requests, but disclosed less-comprehensive data about the number and type of requests they received (F6-F7). **Apple** improved its disclosure but still failed to disclose anything about removing apps from its App Store. While Apple disclosed data on the number of requests it received from different governments to restrict or delete users' accounts, it failed to disclose any similar data about apps it removed from its app store, or the subject matter associated with these removals (F7). According to reports, Apple has removed apps from its App Store in China, Russia, and elsewhere—including the apps for *The New York Times* and LinkedIn,[81] Skype,[82] and hundreds of VPNs—in response to requests from governments.[83]

There were also notable blind spots around companies' handling of private requests. Companies tended to report less information about the number of private requests they received to remove content (F7) compared to those they received from governments (F6). This means users have less information about whether and under what circumstances companies are complying with private requests to censor content or restrict user accounts, or the volume of these types of requests that companies receive.

However, **Twitter, Kakao, Microsoft**, and **Yandex** disclosed more data on private requests than on government requests:

- **Twitter**, for example, disclosed data about the copyright and trademark takedown requests it received, and the number of removals as part of the "EU Trusted Reporters" program to comply with local hate speech laws in Europe. It disclosed the reasons associated with these requests and the number of requests with which it complied.

- **Microsoft** disclosed data on requests to remove information from the Bing search engine, in line with the "Right to Be Forgotten" ruling, as well as removal requests due to alleged copyright infringement. For both of these types of requests, Microsoft disclosed the number of URLs for which it received takedown requests and with which it complied.

- **Kakao** provided data about several different types of private requests, including requests to remove content due to copyright or trademark violations, or defamation. Kakao also listed the number of requests with which it complied.

6.4 Recommendations for companies ## {#section-64}

- **Publish transparency reports that include comprehensive data about the circumstances under which content or accounts may be restricted.** Transparency reports should ideally be published every six months. Information should include:

    - **Government requests to restrict content or accounts:** In particular, companies should disclose the number of requests they receive per country as well as the number of requests with which they comply.

    - **Private requests to restrict content or accounts:** Companies should disclose the volume and nature of requests received, and number complied with, from private individuals or entities not connected to official government or court processes. Companies should also disclose information about the circumstances under which they will respond to private requests, and that they conduct due diligence on such requests.

    - **Priority flagging:** If any organizations or individuals are given special consideration when flagging content for removal as part of informal private processes that do not involve lawful government requests or court orders, these entities should be listed, or at least a description of the process for designating “priority flaggers” should be disclosed. Numbers of requests received from different types of priority flaggers should also be reported, with as much granularity as possible. 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.

    - **Terms of service enforcement:** Companies should disclose the number of actions taken to remove content or restrict accounts that violated the company’s rules, and the reasons for doing so (e.g. the number of accounts restricted for posting extremist content, the number of items removed for containing hate speech, etc.).

- **Provide examples of how rules are enforced:** Even when companies publish their rules, it is very unclear how they are enforced. Reports of arbitrary blocking or inconsistent restrictions on accounts make it all the more difficult to understand how platforms are being policed. Clearer disclosure on this front will help restore trust between users and the services on which they rely, and could help empower users to understand and seek remedy when their content or account has been unfairly restricted.

- **Commit to notify users of censorship events:** Companies should disclose their policies for notifying users when they restrict content or accounts, including the reason for doing so.

5. Privacy failures

Internet and mobile ecosystem companies don’t disclose enough about how they handle user information, which makes it difficult to assess the privacy, security, and human rights risks of using their services.

Internet and mobile ecosystem companies collect vast amounts of information about users. This includes the personal information people give companies when signing up for a service as well as the behavioral data they collect by tracking their browsing activities and preferences, location data, and access and login activities and histories. Such information can be shared with different third parties, including governments, courts, and law enforcement, who make legal demands for user data, and with advertisers. Detailed profiles created with users’ information can be used by government agencies to identify surveillance targets, by financial service companies to determine creditworthiness, and by businesses and other organizations (including advocacy groups and political campaigns), which can target people with advertisements and marketing campaigns tailored to their profiles.[48]

Telecommunications companies also lacked disclosure of how they handle user information. See Chapter 7 for a detailed analysis.

While the misuse and exploitation of information people share with companies does not constitute the type of “breach” or theft discussed in the previous chapter on security (because the information was not technically stolen), the potential for harm to individuals and to vulnerable categories of people is nonetheless very real. Failure to assess and mitigate harm constitutes a betrayal of user trust and lack of respect for user rights.

Reacting to revelations that the political research and consulting firm Cambridge Analytica obtained Facebook user data for the purpose of influencing voters in multiple countries, the Internet Society called it “the natural outcome of today’s data driven economy that puts businesses and others first, not users” and called for “higher standards for transparency and ethics when it comes to the handling of our information. Anyone who collects data must be accountable to their users and to society.”[49]

The Index aims to do just that with seven indicators evaluating corporate transparency about handling of user information.[50] We expect companies to disclose what information they collect (P3), what information they share and the types and names of the third parties with whom they share it (P4), for what purpose they collect and share user information (P5), and for how long they retain this information (P6). Companies should also provide clear options for users to control what information is collected and shared, including for the purposes of targeted advertising (P7), and they should clearly disclose if and how they track people across the internet using cookies, widgets or other tracking tools embedded on third-party websites (P9). We expect companies to clearly disclose how users can obtain all public-facing and internal data they hold on users, including metadata (P8).

Yet 2018 Index results show that users remain largely in the dark about what information about them is collected and shared, with whom, and for what purposes.

What do we mean by "user information"?

RDR defines "user information" as any information that identifies a user's activities, including (but not limited to) 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. Companies might have their own definition of user information, which can differ from RDR's definition of user information and be narrower in scope. For example, a company may define user information as the demographic information a user voluntarily provides upon signing up for a service (e.g., age, gender), but not include automatically collected metadata or other types of information. See the 2018 Index glossary: https://rankingdigitalrights.org/2018-indicators/#userinformation.

5.1. Transparency remains inadequate ## {#section-51}

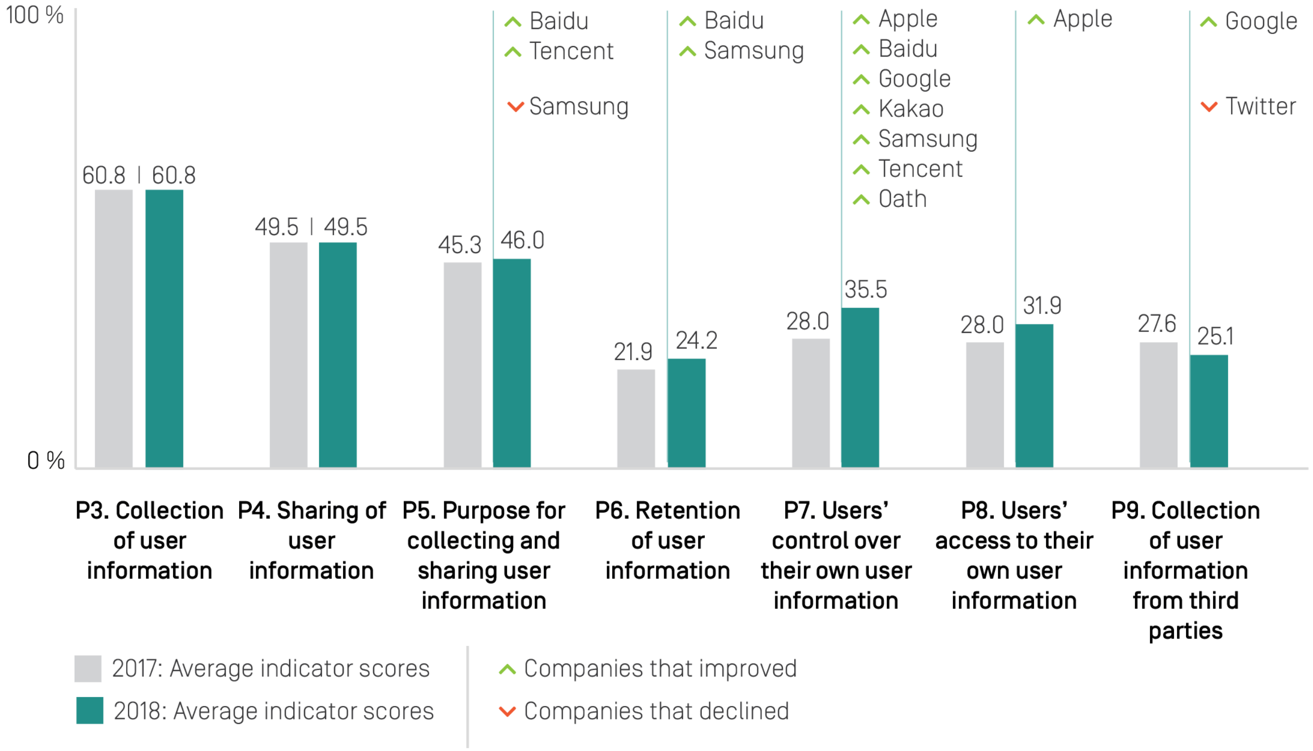
Internet and mobile ecosystem companies have made little progress in disclosing how they handle user information, and what options people have to control what is collected and shared.

As Figure 9 illustrates, internet and mobile ecosystem companies have taken few concrete steps to improve in this area. As a result, users still lack the information they need to make informed choices to assess the privacy and human rights risks they face when using a particular service.

As we found in the 2017 Index, companies in the 2018 index still tended to disclose more about what information they collect, and less about how they manage it. Companies in the 2018 index did not sufficiently disclose what user information they share and with whom, for what purposes they collect and share this information, for how long they retain it, and what options users have to control whether information about them is collected and shared.[51]

While some companies made improvements, all internet and mobile ecosystem companies evaluated still lacked sufficient information about what data they collect (P3) and share (P4), for what purpose they collect and share it (P5), and for how long they retain it (P6) (see Section 5.2). Notably, internet and mobile ecosystem companies disclosed little about their data retention policies. While in some jurisdictions they are legally required to retain user information for specific periods, companies should disclose what that time frame is and whether they retain user information for longer than is legally required. Companies also lacked sufficient information about how users can control what companies collect, and targeted advertising continues to be the default setting (P7) (see Section 5.3).

Figure 9 | How transparent are internet and mobile ecosystem companies about how they handle user information?



- Two companies—Chinese internet companies **Baidu** and **Tencent**—improved their disclosure of reasons for collecting and sharing information (P5), but companies on average scored poorly on this indicator.

- Seven companies—**Apple**, **Baidu**, **Google**, **Kakao**, **Samsung**, **Tencent**, and **Oath**—improved their disclosure of options users have to control their own information (P7), but disclosure of these options still remains unsatisfactorily low (see Section 5.3).

- Just one company—**Apple**—improved its disclosure of options users have to access their information (P8).

- **Google** improved its disclosure of whether and how it tracks Android users across the internet (P9), clarifying that it may use tools similar to cookies to present users of mobile applications and browsers with tailored advertising, and explained the reasons for doing so.[52]

- Revisions in **Twitter's** privacy policy made its policies and practices about its tracking of users across the internet less clear (P9). Notably, Twitter also disclosed it does not respect Do Not Track (DNT) signals that allow users to indicate they do not want to be tracked across the internet (see Section 5.4).

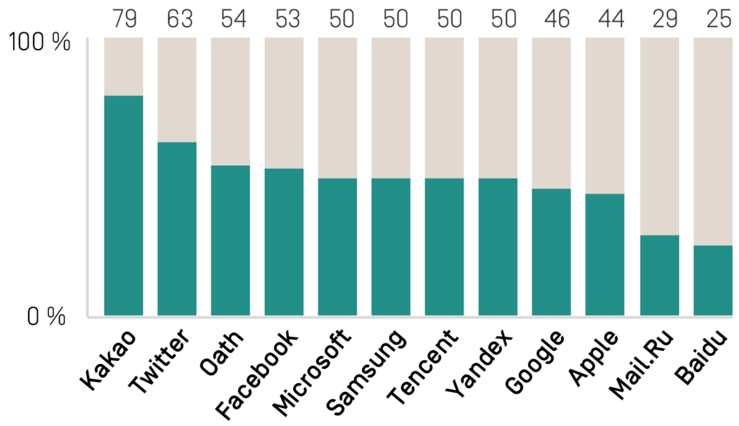
5.2. What, whom, and why? ## {#section-52}

Internet and mobile ecosystem companies don’t disclose enough about what information they are sharing, with whom, or for what purpose.

The Index includes two indicators that evaluate how transparent companies are about their data-sharing policies (P4, P5). Indicator P4 evaluates company disclosure of what user information companies share, including the types and names of third-parties with whom they share it. Indicator P5 evaluates whether and how clearly companies disclose their purpose for collecting and sharing user information.

As shown in Figure 10, most internet and mobile ecosystem companies did not sufficiently disclose what types of information they share and with whom, with only two of the 12 companies scoring more than 50 percent on this indicator (P4). **Kakao’s** disclosure on this indicator far surpassed all others. Notably, **Google** and **Apple** disclosed less about their data-sharing practices than most internet and mobile ecosystem companies evaluated, only scoring higher on this indicator than **Mail.Ru** and **Baidu**, which were among the lowest scoring companies in the Index overall.

Figure 10 | How transparent are internet and mobile ecosystem companies about what user data they share and with whom [P4]?

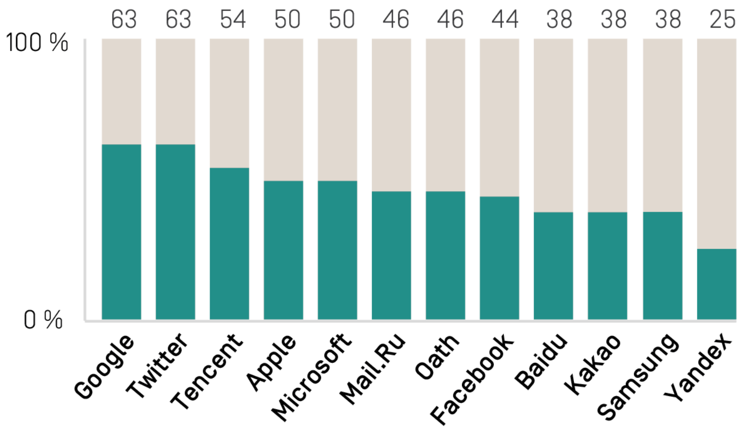


Indicator P4 evaluates company disclosure of what user information they share, including the types and names of third-parties with whom they share it. See: *https://rankingdigitalrights.org/index-2018/indicators/p4*

An examination of element-level data for this indicator (P4) revealed that while all internet and mobile ecosystem companies disclosed a policy of sharing user information with government authorities if requested, they were less transparent about what other types of third parties they share information with and what types of user information they share. Only a handful of companies disclosed the actual names of third parties with whom they share user information, and no company disclosed all the types of user information they share. Likewise, mobile ecosystem companies did not sufficiently disclose whether they review the data-sharing practices of the apps hosted in their app stores.

Internet and mobile ecosystem companies disclosed even less about why they collect and share user information, with an average score of 46 percent on this indicator (P5, Figure 11). However, the order of the ranking on this indicator looks very different than for Indicator P4, with Google and Twitter tied at the top. But their top score of 63 percent leaves much room for improvement. Notably, Facebook disclosed substantially less about reasons for collecting and sharing user information than its U.S.-based peers.

Figure 11 | How transparent are internet and mobile ecosystem companies about the purpose for collecting and sharing user information (P5)?



Indicator P5 evaluates if and how clearly companies disclose the purpose for collecting and sharing user information. See: *https://rankingdigitalrights.org/index-2018/indicators/p5*

An analysis of element-level disclosure on this indicator shows that while many companies disclosed whether they combine user information from different services and the reasons for doing so, fewer disclosed their reasons for collecting and sharing user information. Companies were particularly hesitant to make a clear commitment to using information only for the purposes for which it was collected.

For more information and data:

- P4: https://rankingdigitalrights.org/index2018/indicators/p4
- P5: https://rankingdigitalrights.org/index2018/indicators/p5

5.3. Targeted advertising and lack of user control ## {#section-53}

Users lack clear options to control what companies collect and share about them, including for targeted advertising.

Recent examples of harmful content and misinformation targeted at social media users illustrate that pervasive user tracking not only poses threats to privacy and security, but also to the basic functions of open democracy.[53] Therefore, it is critical that people have control over what information about them is collected and shared, including how this information is used to target them for commercial and political advertising. Targeted advertising involves tracking users extensively and retaining large amounts of information on them.[54] Companies should therefore clearly disclose whether users have options to control how their information is being used for these purposes.

Indicator P7 evaluates company disclosure of what options users have to control what information the company collects on them and uses, including for the purposes of targeted advertising.[55] We expect companies to allow users to control what information is collected about them, which also means enabling users to delete specific types of information without requiring them to delete their entire account. In addition, we expect companies to give users options to control how their information is used for advertising and to disclose that targeted advertising is off by default.

Options users have to control what is collected about them

Indicator P7 contains four elements measuring how transparent companies are about giving users options to control what information about them is collected and used, including for targeted advertising.

- **Element 1: Does the company clearly disclose whether users can control the company's collection of this user information?** Companies should allow users to control what information about them is collected.

- **Element 2: Does the company clearly disclose whether users can delete this user information?** Giving users control over what information about them is collected about them means companies should give users the ability to delete specific types of user information.

- **Element 3: Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?** Companies should clearly disclose whether users have options to control how their information is being used for these purposes.

- **Element 4: Does the company clearly disclose that targeted advertising is off by default?** Companies should clearly disclose that targeting advertising is off by default.

See the 2018 Index at: https://rankingdigitalrights.org/2018-indicators/#P7.

The 2018 Index data showed that most companies failed to disclose clear options for users to control what data about them is collected and how it is used for the purposes of advertising (Figure 12). While a majority of internet and mobile ecosystem companies improved their disclosure on this indicator, disclosure of these options remained insufficient.

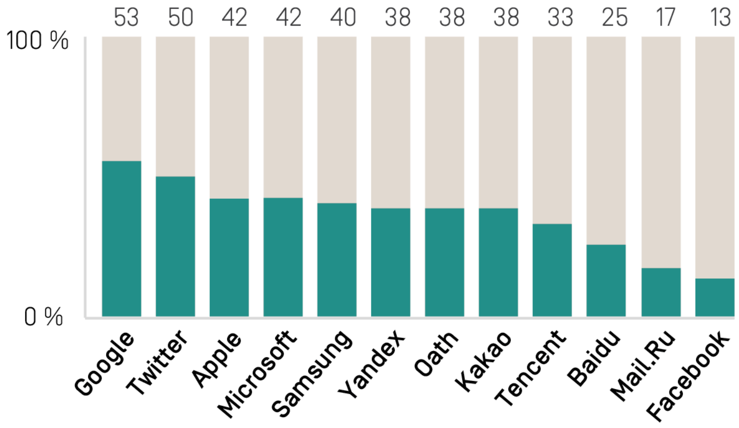
- Seven companies—**Apple**, **Baidu**, **Google**, **Kakao**, **Samsung**, **Tencent**, and **Oath**—improved their disclosure of options users have to control their information, which includes options to control if and how their data is collected for targeted advertising (P7) (See company report cards for details.)

- **Google** was the most transparent among internet and mobile ecosystem companies on this particular indicator. In addition to giving users limited options to control the collection of their information and to delete some of this information, the company explained how users can opt out of targeted advertising. However, it appeared from this disclosure that targeted advertising is on by default.

- **Facebook** disclosed the least on this topic. The company did not clearly disclose whether users can control the collection of their information, and it also did not disclose whether users are able to delete some of this information. Despite giving users limited options to control how their information is used for advertising purposes, the company failed to commit to turn off advertising by default.

- **Twitter** disclosed less than Google on this indicator, but was on par with Apple's disclosure. Twitter disclosed that it allowed users to control the collection of some of their information and delete some of this information, but did not disclose whether this was the case for all types of user information the company collects. Like most other internet and mobile ecosystem companies evaluated, Twitter explained how users can control whether their information is used for advertising purposes, but it did not indicate that interest-based advertising was off by default.

Figure 12 | How transparent are internet and mobile ecosystem companies about options users have to control their own data (P7)?



Indicator P7 evaluates company disclosure of options users have to control what information about them is collected and used, including for targeted advertising. See: *https://rankingdigitalrights.org/index-2018/indicators/p7*

User privacy should be the default.

In order to provide users with free services, many internet and mobile ecosystem companies monetize the information they hold about their users. Advertising technologies allow companies and third parties to target users based on profiles derived from this data. Given the significant privacy implications of targeted advertising, companies should provide users with control over how their information is used for targeted advertising. Moreover, companies should not assume that all users have an understanding of the privacy concerns resulting from these advertising practices. Therefore, targeted advertising should be *off* by default.

What is targeted advertising?

Targeted advertising, also known as “interest-based advertising” or “personalized advertising,” refers to the practice of collecting a range of data about individual users—including demographic data, browsing history and preferences, and location information—with the goal of personalizing the ads users see online. Typically, targeted advertising relies on vast data collection practices, which can involve tracking users’ activities across the internet using cookies, widgets, and other tracking tools, in order to create detailed user profiles.

What do we mean by opting out versus opting in?

“Opt-in” means the company does not collect, use, or share data for a given purpose until users explicitly signal that they want this to happen. “Opt-out” means the company uses the data for a specified purpose by default, but will cease doing so once the user tells the company to stop.

For more:

- Ghosh, Dipayan and Ben Scott, “Digital Deceit: The Technologies Behind Precision Propaganda on the Internet,” New America, January 2018, https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/.

- See the 2018 Index glossary at: https://rankingdigitalrights.org/2018-indicators/#optionstocontrol.

Despite significant public concerns regarding the invasive nature of of social media platforms’ advertising tools, **Facebook** provided users with only limited options to control the use of their information for targeted advertising. Furthermore, for both Facebook, the social networking platform, and Facebook’s Messenger service, the company disclosed that it may always use information such as age and gender to present users with advertising.[56]

Mail.Ru disclosed slightly more than Facebook regarding the options users have to control the collection of their information and to delete some of it. At the same time, the Russian company was the only internet and mobile ecosystem company not to reveal anything about how users can control the use of their information for advertising purposes.

Most internet and mobile ecosystem companies clearly disclosed at least some options users have to control how their information is used for targeted advertising, implying it is *on* by default. None disclosed that targeted advertising was *off* by default.

5.4. Tracking users ## {#section-54}

All mobile ecosystems—Apple iOS, Google Android, and Samsung's Android—disclosed options to control location tracking.

Geolocation data collection is critical to the functionality of many mobile applications, but it can also raise significant concerns for user privacy. This information is particularly sensitive as many users take their devices wherever they go, oftentimes not keeping in mind that they are being tracked. For those who are part of vulnerable communities, including journalists, sexual minorities, and human rights activists, location data tracking can also result in physical harm.

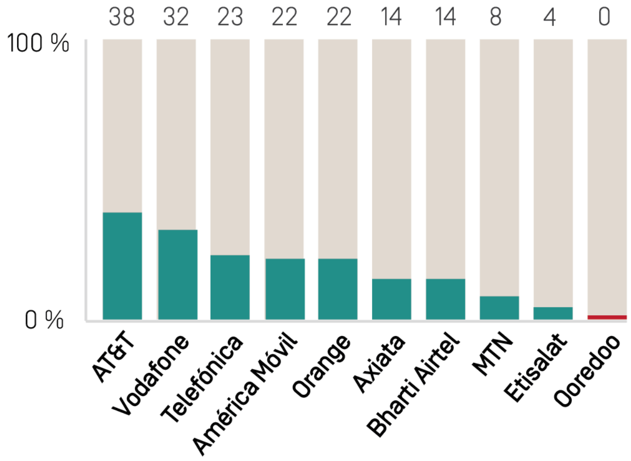
For these reasons, we expect companies to disclose that users can control geolocation data tracking. Users should be able to control geolocational data tracking at the device level, as well as on an app-by-app basis. This enables them to determine whether device manufacturers and individual applications can access this data. All three mobile ecosystems evaluated in the 2018 Index clearly disclosed options for users to turn off geolocation data collection. While **Apple** and **Google** provide user control at both the device level and on an app-by-app basis, **Samsung** only disclosed how users can control this information at the device level.

Most internet and mobile ecosystem companies don't disclose if and how they track people across the web.

Internet and mobile ecosystem companies not only collect information about what people do when using their services, but they also track users' web browsing activities. Indicator P9 evaluates how transparent internet and mobile ecosystem companies are about these practices, looking for companies to disclose if, how, and why they track people across third-party websites.[57] We expect companies to disclose what types of information they collect via cookies, widgets, and other types of trackers, the purposes for doing so, and how long they retain this information. We also expect companies to disclose if they respect "Do Not Track" signals, which allow users to tell companies not to collect or store information about their visits to or activities on third-party websites.[58]

Results of the 2018 Index show that all companies other than **Apple** lacked sufficient disclosure regarding whether and how they track users across the internet (Figure 13). **Apple was the only company that clearly stated it does not track users on third-party websites.** The remaining 11 internet and mobile ecosystem companies in the Index either lacked clear disclosure about their tracking practices or provided no information at all.

Figure 24 | How transparent are telecommunications companies about their handling of user information [P3-P8]?



Average scores for Indicators P3-P8, evaluating corporate disclosure of: what user information they collect [P3], share [P4], the purpose for doing so [P5], for how long they retain it [P7], options they give users to control what is collected, including for the purposes of targeted advertising [P7], and options users have to obtain all of the information the company holds on them [P8]. See: *https://rankingdigitalrights.org/index-2018/indicators*

- **Google** made slight improvements to its disclosure by more clearly explaining how it tracks users of the Android mobile ecosystem. It clarified that it may use tools similar to cookies to present users with targeted advertising, and it explained reasons for doing so.

- **Twitter** became less transparent about how long it retains the information it collects by tracking users and its purposes for collecting it.

- **Facebook's** disclosure of user tracking on third-party sites and services was also unclear. For Facebook, the social network, and Messenger, the company disclosed what information it collects about users on third-party websites with tracking tools like cookies and widgets, but it did not disclose the purpose for doing so, or for how long it retains this information. For Instagram and WhatsApp, Facebook did not disclose whether, how, or for what purpose it tracks users on third-party websites.

- None of the companies disclosed that they respect user-generated signals to opt out of data collection. Three companies—**Microsoft**, **Oath** and **Twitter**—explicitly stated they do not respect "Do Not Track" signals from users asking companies not to track them across the web.[59] The remaining companies did not indicate whether they respect such signals.

- **Baidu** and **Mail.Ru** were among several companies that did not provide any information on whether they track users across the web.

5.5. Recommendations for companies ## {#section-55}

- **Maximize user control over their own data.** Companies should not only provide clear disclosure of how they handle user information, but also give users clear options to control what information is collected and shared and with whom. This should also include user control over whether their information is combined from different company services.

- **Ensure transparency around handling of user information.** Companies should clearly disclose how they handle users' information, including what information is collected and shared, as well as the purposes for doing so. Companies should disclose:

    - what specific types of information they collect (P3);

    - how that information is collected (e.g., does a company ask users to provide certain information, or does the company collect it automatically?) (P3);

    - what information is shared and with whom (P4);

    - why they collect and share that information (P5);

    - how long the information is retained (P6);

    - whether and how the that information is destroyed when users delete their accounts or cancel their service (P6);

    - whether—and the extent to which—users can control what information about them is collected and used (P7); and

    - whether users can access all public- facing and private information a company holds about them (P8).

- **Tell users whether and how they are tracked.** Companies should clearly disclose whether and how they collect user information from third-party sites and services.

- **Facilitate user access to their information.** Users should have the ability to obtain all the information a company holds about them, and to download it in a format that allows them to transfer some or all of this data into a new service, if they wish to do so.

- **User privacy should be the default.** Companies should not assume that users are aware of the connection between data collection and targeted advertising, and targeted advertising should be off by default.

- **Respect user preferences.** Companies should support the development of a viable system for users to indicate they do not want to be tracked across the internet, and make a clear commitment to respect these preferences.

- **Build partnerships for stronger user privacy.** Companies should proactively and systematically engage with researchers, engineers and advocates to ensure company policies and practices reflect privacy best practices.

- **Privacy innovation.** Invest in the development of technologies and business models that maximize user control over their personal information and content.

9. Questions for investors

The Ranking Digital Rights Corporate Accountability Index data and methodology offer a useful framework for investors to evaluate whether companies have made best efforts to mitigate risks to their business by working to anticipate and reduce potential harms to those who use their technologies, platforms, and services. Such risks are not limited to traditional “cybersecurity” threats related to hacking and data breaches. Shareholder value is also put at risk when companies fail to identify and mitigate broader risks to user privacy across their business operations, or fail to anticipate and address content-related issues spanning from hate speech and disinformation to government censorship and network shutdowns.[107]

The following ten questions can help investors evaluate whether companies are making adequate efforts to respect users’ rights, thereby mitigating individual harms and broader business risks. These questions are also a useful starting point for investor engagement with companies, particularly when combined with key findings and recommendations from the individual company report cards.

1. **Risk assessment:** Has the company management identified digital rights risks that are material to its business and does the company carry out impact assessments on the full range of these risks? Does it disclose any information about whether and how the results of assessments are used?

2. **Oversight:** Does the board exercise direct oversight over risks related to user security, privacy, and freedom of expression? Does board membership include people with expertise and experience on issues related to digital rights?

3. **Stakeholder engagement and accountability:** Is the company a member of the Global Network Initiative (GNI) and if not, why not?

4. **Transparency about data collection and use:** Does the company disclose clear information about its policies and practices regarding collection, use, sharing, and retention of information that could be used to identify, profile or track its users?

5. **Transparency about handling of government demands and other third party requests affecting users’ expression and privacy rights:** Does the company disclose policies for how it handles all types of third-party requests (by authorities or any other parties) to share user data, restrict content, restrict access, or shut down service (including network shutdowns by telecommunications companies)?

6. **Transparency reporting:** Does the company publish data about the volume and nature of the requests it receives, and responds to, for: sharing user data, restricting content or accounts, shutting down networks? Does it also publish data about the volume and nature of content and accounts restricted in the course of enforcing its own terms of service?

7. **Evidence of strong policies for addressing security vulnerabilities:** Does the company

disclose clear information about policies for addressing security vulnerabilities, including the company’s practices for relaying security updates to mobile phones?

8. **Encryption:** Does the company commit to implementing the highest encryption standards available for the particular product or service? If not, why not?

9. **Mobile security:** Do companies that operate mobile ecosystems disclose clear policies about privacy and security requirements for third-party apps?

10. **Telecommunications transparency about network management:** Do telecommunications companies disclose whether they prioritize, block, or delay applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network? If yes, do they disclose the purpose for doing so?

9. Questions for investors to ask

The Ranking Digital Rights Corporate Accountability Index data and methodology offer a useful framework for investors to evaluate whether companies have made best efforts to mitigate risks to their business by working to anticipate and reduce potential harms to those who use their technologies, platforms, and services. Such risks are not limited to traditional "cybersecurity" threats related to hacking and data breaches. Shareholder value is also put at risk when companies fail to identify and mitigate broader risks to user privacy across their business operations, or fail to anticipate and address content-related issues spanning from hate speech and disinformation to government censorship and network shutdowns.[107]

The following ten questions can help investors evaluate whether companies are making adequate efforts to respect users' rights, thereby mitigating individual harms and broader business risks. These questions are also a useful starting point for investor engagement with companies, particularly when combined with key findings and recommendations from the individual company report cards.

1. **Risk assessment:** Has the company management identified digital rights risks that are material to its business and does the company carry out impact assessments on the full range of these risks? Does it disclose any information about whether and how the results of assessments are used?

2. **Oversight:** Does the board exercise direct oversight over risks related to user security, privacy, and freedom of expression? Does board membership include people with expertise and experience on issues related to digital rights?

3. **Stakeholder engagement and accountability:** Is the company a member of the Global Network Initiative (GNI) and if not, why not?

4. **Transparency about data collection and use:** Does the company disclose clear information about its policies and practices regarding collection, use, sharing, and retention of information that could be used to identify, profile or track its users?

5. **Transparency about handling of government demands and other third party requests affecting users' expression and privacy rights:** Does the company disclose policies for how it handles all types of third-party requests (by authorities or any other parties) to share user data, restrict content, restrict access, or shut down service (including network shutdowns by telecommunications companies)?

6. **Transparency reporting:** Does the company publish data about the volume and nature of the requests it receives, and responds to, for: sharing user data, restricting content or accounts, shutting down networks? Does it also publish data about the volume and nature of content and accounts restricted in the course of enforcing its own terms of service?

7. **Evidence of strong policies for addressing security vulnerabilities:** Does the company

disclose clear information about policies for addressing security vulnerabilities, including the company’s practices for relaying security updates to mobile phones?

8. **Encryption:** Does the company commit to implementing the highest encryption standards available for the particular product or service? If not, why not?

9. **Mobile security:** Do companies that operate mobile ecosystems disclose clear policies about privacy and security requirements for third-party apps?

10. **Telecommunications transparency about network management:** Do telecommunications companies disclose whether they prioritize, block, or delay applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network? If yes, do they disclose the purpose for doing so?

8. Recommendations for governments

Even in the absence of policy and regulatory reform, all companies in the Index can take immediate steps to improve their respect for users' rights. Yet the 2018 Index results also highlight the extent to which government, law, and politics shape companies' ability to respect users' freedom of expression and privacy. The rights of internet users around the world will be better protected and respected if governments take the following measures:

Privacy: Enact and enforce comprehensive data protection laws in consultation with industry and civil society, with impact assessments to ensure that the laws can avoid unintended consequences for freedom of expression.

Such laws should:

- **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.

- **Require companies to implement and disclose appropriate policies and procedures for handling data breaches,** and to notify users when their data has been compromised.

Security: Support appropriate incentives for companies to adopt industry standard security practices and require appropriate disclosure to users.

Research and Development: Support development of technologies and business models that maximize individual control over personal data as well as the information and content that people create. Most immediately, support development of a viable system for users to indicate they do not want to be tracked across the internet, and establish incentives for companies to make a clear commitment to respect these preferences.

Corporate accountability: Ensure that laws and regulations maximize companies' ability to be transparent and accountable with users about how they receive and handle government and other third-party requests to restrict speech or information flows, or to share user information. Laws that prevent transparency and cannot be justified on public security grounds, in line with international human rights standards, should be reformed.

Government accountability: 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.[101]

Judicial remedy: Ensure that adequate judicial remedies are in place for internet users whose freedom of expression and privacy rights are violated.

Corporate remedy: Require companies to provide and 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 a company's products and services.

Legislative accountability: 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[102] and international human rights instruments, such as the International Covenant on Civil and Political Rights.[103] Where laws are not compatible with human rights standards, reform should include:

- **Surveillance reform: Reform surveillance-related laws** and practices to comply with the thirteen "Necessary and Proportionate" principles,[104] a framework for assessing whether current or proposed surveillance laws and practices are compatible with international human rights norms.

- **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.[105]

- **Protect 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.

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

4. Security uncertainty

Companies lack transparency about what they do to safeguard users' data, which means people don't know the security, privacy, and human rights risks they face when using a particular platform or service.

People entrust internet, mobile, and telecommunications companies with enormous amounts of personal information. Weak security safeguards can lead to theft or malicious exposure of this information. Companies that wish to earn and maintain user trust—and mitigate material risks to their business—should demonstrate a commitment to keeping user information secure.

The 2018 Index contains three indicators (P13, P14, P15) evaluating company transparency about what internal steps they take to keep user information secure. Companies should disclose basic information about their own internal security policies so that users can better understand the risks of using their products and services, and make informed decisions about how to use them safely.

The Index also includes three additional security indicators evaluating company disclosure of encryption policies and practices (for internet and mobile ecosystem companies) (P16), company disclosure of what users can do to keep their accounts secure (P17), and company disclosure of materials aimed at educating users about how they can protect themselves from cybersecurity risks (P18). Companies made few substantive changes to their disclosure of the security issues addressed in these indicators. More information on how companies performed on these indicators can be found at: https://rankingdigitalrights.org/index2018/

4.1. Disclosure failure ## {#section-41}

Companies fail to communicate basic information about what they are doing to keep users' information secure.

Results of the 2017 Index showed that companies tended to communicate more about what users can do to protect their own information than about what the companies themselves do to keep user data secure.[36] The 2018 Index data shows that companies have made little progress in this area.

Despite the rise in data breaches reported in the media, and growing concerns about how companies keep the vast amount of data they hold on users secure, companies across the board lacked clear and consistent disclosure of steps they take to safeguard data that they collect and store. While internet and mobile ecosystem companies disclosed more than telecommunications companies about their internal security measures, all companies fell short of providing enough information for users to know what policies and practices are in place to keep their information secure (Figure 5).

![figure5](/assets/graphics/content/Figure 5. How transparent are companies are about their internal security measures (P13-P15)_.png "figure5")

The 2018 Index data revealed the following trends:

- **Few companies communicate their policies for handling data breaches.** Most companies failed to provide any information at all about how they respond to data breaches (P15). While two of 22 companies—Apple and Vodafone—improved, and Vodafone was the only company to receive a full score on that indicator, most companies still failed to disclose even basic information about what procedures they have in place to respond to data breaches in the event that such incidents occur (see Section 4.2).
- **Companies do not communicate enough information about security oversight practices.** Data showed that companies lacked transparency about their security oversight procedures, including whether they limit employee access to user information. While all companies tended to disclose some information about their oversight procedures, most still fell short of clearly communicating to users what steps they take to keep their information secure (P13) (see Section 4.3).
- Nonetheless, five companies—Airtel India (Bharti Airtel)**,** Celcom (Axiata)**,** Etisalat UAE**,** Orange France**,** and Tencent—improved their disclosure of security oversight policies and practices (P13). Celcom (Axiata) and Orange France both made clearer commitments to conduct security audits, and Airtel India (Bharti Airtel) and Etisalat UAE published more detailed information about steps they take to limit and monitor employee access to user information. Tencent also clarified how the company limits employee access to WeChat user information, though it did not disclose any mechanisms in place to ensure these policies are enforced.
- **Companies lacked clarity about how they handle security vulnerabilities.** While internet and mobile ecosystem companies were more transparent than telecommunications companies about their processes for addressing security vulnerabilities, all companies lacked clarity about their policies and processes (P14). No company made any improvements to their disclosure of their approaches to dealing with security vulnerabilities in the 2018 Index (see Section 4.4).

4.2. Handling of data breaches ## {#section-42}

Most companies failed to disclose policies for responding to data breaches, including whether they would notify those affected.

Data breaches not only expose users to financial crimes committed by malicious hackers and cybercriminals, but other actors can exploit such breaches against at-risk communities. For example, a data breach affecting an email-service provider can expose the communications and sources of human rights activists and investigative journalists to government authorities in repressive regimes.

Companies should immediately respond to data breaches when they occur. Indicator P15 evaluates if companies disclose a commitment to notify relevant authorities and potentially affected users in the event of a breach, and if they clearly disclose what kinds of steps they will take to address the impact on users.[37] Notifying the authorities without undue delay allows officials to immediately investigate a breach, find the perpetrators, and bring them to justice. Notifying victims of breaches can help them take the necessary precautions to protect themselves, such as by changing their passwords, warning their contacts, and securing financial accounts.

However, while many jurisdictions legally require companies to notify relevant authorities or take certain steps to mitigate the damage of data breaches, companies may not necessarily be legally compelled to disclose this information to the public or affected individuals. For example, telecommunications companies in India are required to notify authorities of a data breach,[38] but there is no regulatory requirement to notify victims.

Even if there is a legal requirement to notify affected individuals, the exact definition of “affected individuals” can also vary significantly in different jurisdictions. However, regardless of whether the law is clear or comprehensive, companies that respect users’ rights should clearly disclose when and how they will notify individuals who have been affected, or have likely been affected, by a data breach.

Communicating about data breaches: What do we expect companies to disclose? Indicator P15 contains three elements evaluating company disclosure of policies for responding to and communicating about data breaches.

- **Element 1: Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?** Legally, companies are often required to notify the relevant authorities when a data breach occurs. This element does not focus on whether companies disclose the specifics of which authorities they will notify, since this may vary from jurisdiction to jurisdiction, but rather whether companies commit to notify the designated authority as soon as possible.
- **Element 2: Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?** Companies should commit to notifying affected individuals as soon as possible and fully disclose what information of theirs was exposed.
- **Element 3: Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?** Although a company’s specific response will vary depending on the nature of the breach, the company should provide examples of what kinds of steps it will take internally to secure its data and commit to notifying affected individuals of steps they can take to mitigate risk or damage. See 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P15.

Since the 2017 Index there has been only minor progress. Apple joined AT&T, Telefónica, and Vodafone as the only companies to disclose any information about their policies and practices for responding to data breaches.

![figure6](/assets/graphics/content/Figure 6. How transparent are companies about policies for responding to data breaches (P15)_.png "figure6")

As Figure 6 illustrates, most of the 22 companies in the Index failed to provide basic information about their policies for responding to data breaches:

- Vodafone was the only company to receive full credit on this indicator. The company disclosed a

policy of notifying authorities without undue delay when a data breach occurs, and of notifying data subjects who might be affected. The company also clearly explained the steps taken to address the impact of a data breach on its users.
- Apple was the only internet and mobile ecosystem company to provide any information about policies for responding to a data breach. It was the only company aside from Vodafone to disclose any information about notifying authorities.
- All four companies—Apple, AT&T, Telefónica, and Vodafone—disclosed some information about their policies for notifying individuals affected. But only Apple, Telefónica, and Vodafone disclosed information about the steps they would take to address the impact of a data breach on users.

4.3. Security oversight ## {#section-43}

Most companies lack transparency about their security oversight policies and practices, including whether they limit employee access to user information.

While most data breaches can and do occur as a result of malicious actors and external threats, many also stem from poor internal security oversight.[39] Research shows that the security issues posed by so-called “insider threats” are as serious a problem as those posed by external threats.[40]

Good internal security practices therefore include restricting and monitoring unauthorized access to user information by employees. Companies should also conduct regular security audits to ensure that company security practices are properly implemented, that all software and systems are up-to-date, and that potential security vulnerabilities are addressed. A robust security audit program includes both internal and third-party audits, which can help to ensure that a company is not only meeting its own security standards but also following industry best practices.

Indicator P13 evaluates company disclosure of security oversight policies and practices for safeguarding user data.[41] We expect companies to disclose basic information on what steps they take internally to keep user information secure, including if they limit and monitor employee access to user information, and whether they conduct internal and external security audits on products and services. While we do not expect companies to disclose sensitive information that would undermine the security of these systems, or that would expose them to attacks, we do expect each company to disclose basic information about how these oversight systems function, so it is clear that the company has strong security processes in place.

![figure7](/assets/graphics/content/Figure 7. How transparent are companies are about their security oversight processes (P13)_.png "figure7")

Figure 7 illustrates a wide range in companies’ disclosure about security oversight processes. Notably:

- Among internet and mobile ecosystem companies, **Google** and **Kakao** earned full credit for disclosure of their security oversight processes, with each providing clear information about limiting and monitoring employee access to user information, conducting internal security audits, and commissioning third-party audits on their products and services.
- **AT&T** was the only telecommunications company to earn full credit, disclosing more than Vodafone UK, Orange France, and Telefónica Spain. The company disclosed that it conducts regular internal and external security reviews, and mentions safeguards it has in place, including limiting employee access to personal information and requiring an employee username and password to access sensitive information.[42]

- Just six companies—**AT&T, Bharti Airtel, Google, Kakao, Samsung,** and **Vodafone**—clearly disclosed that they limit and monitor employee access to user information. Six other companies, including Facebook and Twitter, failed to indicate if they have processes in place to prevent unauthorized access to user information.
- While most companies disclosed some information about internal security audits they conduct on their products and services, just four companies—**AT&T, Google, Kakao,** and **Twitter**—reported commissioning third-party security audits.

4.4. Identifying and addressing vulnerabilities ## {#section-44}

Companies lacked adequate information about how they address security vulnerabilities when they are discovered.

No security system is infallible. Even with rigorous security oversight practices in place, it is not uncommon to find vulnerabilities in a company's products and services—which, if exploited, could put their users' personal information at risk.

Indicator P14 evaluates company disclosure of how they address security vulnerabilities and what actions they take to mitigate those that they discover.[43] We expect companies to disclose that they have a program, such as a "bug bounty" to reward security researchers for alerting them to security vulnerabilities in their products. Telecommunications and mobile ecosystem companies are expected to disclose if they have made modifications to a mobile operating system and how that might affect security updates. Mobile ecosystem companies should disclose how they ensure the security of software updates and for how long they will continue to provide these updates for their operating system and other software.

As Figure 8 illustrates, all companies lacked clear disclosure of how they address security vulnerabilities.

![figure8](/assets/graphics/content/Figure 8. How transparent are companies about their policies for addressing security vulnerabilities (P14)_.png "figure8")

Among internet and mobile ecosystem companies, **Facebook, Yandex,** and **Tencent** disclosed more information about how they address security vulnerabilities than their peers, although all of these companies still fell short. **Google** disclosed a security vulnerabilities reward program, but did not disclose a timeframe for responding to reports submitted for Gmail, Search, or YouTube, and did not commit to not pursue legal action against security researchers. It also failed to commit to provide security updates for its Android operating system for at least five years after release. Notably, **Apple** revealed less than Chinese internet company **Baidu**—one of the least transparent companies in the Index overall—about its approach to handling vulnerabilities it discovers.

Just two telecommunications companies—**AT&T** and **MTN**—disclosed anything about policies and practices for addressing security vulnerabilities. Notably, no telecommunications company evaluated disclosed whether they make modifications to a mobile phone's operating system.

Telecommunications companies and mobile phone manufacturers can make updates to the Android operating system code that may also delay when users can receive security updates from Google. **Samsung** is the only mobile ecosystem company evaluated that adapts for use in its devices an operating system released by another company (Samsung's implementation of Google's Android). It did not disclose a specific timeframe in which it committed to implement security updates released by Google Android. None of the telecommunications companies disclosed a specific timeframe in which mobile operating system security updates are delivered to users.

As noted in the 2017 Index report, the timely delivery of security updates is not only a security issue, but also a social equity issue, as newer and more expensive smartphones are more likely to be up-to-date than older and less expensive models, which means lower income populations can face greater security risks.[44] It is therefore crucial that companies commit to provide security patches within one month of a vulnerability being announced to the public.

4.5. Spotlight: "Bug bounties" and reporting vulnerabilities ## {#section-45}

Companies can benefit from the knowledge and skills of others, including security researchers and ethical hackers, who can identify security vulnerabilities that a company may not be aware of. If unknown to the company, security vulnerabilities can be exploited by criminals or oppressive governments seeking to spy on their citizens. In August 2016, for example, researchers at Citizen Lab identified and alerted Apple to a security vulnerability in its software that had been used to target journalists and activists in the UAE, Mexico, and elsewhere.[45] Security vulnerability reporting mechanisms are a valuable way for companies to add an extra layer of security review for their products and to demonstrate a strong commitment to user security.

By outlining clear processes for researchers to submit security vulnerabilities, companies can ensure that these reports reach the right people in a timely manner. Offering positive recognition and financial rewards ("bug bounty") is a way to further incentivize security researchers by recognizing their work, and to demonstrate that the company values these reports as part of implementing its commitment to user security.

What is a bug bounty program?

A bug bounty program is one example of a security vulnerability reporting mechanism that allows security researchers to submit "bugs," or code errors, with an emphasis on reporting security vulnerabilities that can be exploited. Bug bounty programs recognize and reward researchers for submitting these vulnerabilities, including with financial compensation. In the absence of a clearly defined vulnerability reporting mechanism such as a bug bounty program, individuals may not know how, or if, they can report these issues to the company. This is a security liability: vulnerabilities can remain unpatched and can be exploited if discovered by malicious actors. Lack of a clear policy could also expose individuals to criminal charges of hacking or computer crimes simply for making a good faith effort to report security issues.[46] Lawsuits against journalists and security researchers for reporting vulnerabilities can also deter individuals from reporting security vulnerabilities to a company for fear of being sued or criminally charged.[47] If a company does not commit not to pursue legal charges, individuals may be discouraged from notifying a company of vulnerabilities, even through its disclosed reporting mechanism. **Further reading:** Andi Wilson, Ross Schulman, Kevin Bankston, and Trey Herr, “Bugs In the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications,” Open Technology Institute, July 2016, https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf.

Index data showed that all internet and mobile ecosystem companies in the 2018 Index disclosed some type of mechanism allowing researchers to report security vulnerabilities, although these programs ranged in their accessibility and comprehensiveness.

Some companies provided only an email address for researchers to submit vulnerability reports, while others offered more robust bug bounty programs that included monetary rewards and public recognition for reports submitted within the scope of the program. **Facebook** was the only company to commit not to pursue legal action against researchers who report vulnerabilities through its reporting mechanism. **AT&T** was the only telecommunications company to disclose a bug bounty program, although it did not clearly disclose a timeframe in which the company will review reports, or commit to refrain from pursuing legal action against those who submit such reports.

4.6. Recommendations for companies ## {#section-46}

- **Disclose how data breaches are handled.** Companies should disclose policies for responding to data breaches. This includes making a commitment to notify the authorities without undue delay, explaining how they will notify individuals who may have been impacted, and outlining what kind of steps they will take to address and minimize the breach’s impact.
- **Explain internal processes for safeguarding user information.** This includes disclosing that systems are in place to both limit and monitor employee access to user information, that an internal security team conducts security audits on the company's products and services, and that the company also commissions third-party security audits on its products and services.
- **Provide a mechanism for individuals to report vulnerabilities to the company.** Companies should clearly outline how security researchers can submit vulnerabilities they discover, and explain any rules they may have for these programs. Companies should also commit not to pursue legal action against individuals who submit reports of vulnerabilities within the scope of these programs.
- **Address security vulnerabilities when they are discovered.** Companies should clearly disclose the timeframe in which they will review reports of vulnerabilities. Mobile ecosystem companies and telecommunications companies that use operating systems adapted from other companies’ operating systems, such as Android, should commit to provide security patches within one month of a vulnerability being announced to the public.
- **Where permitted by law, publicly commit to implement the highest encryption standards available.** This disclosure should include encryption in transit and at rest, end-to-end encryption, and forward secrecy. At minimum, companies should 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, companies should clearly say so to users, explaining the specific legal barrier and the potential consequences for user privacy and safety.

7. Telecommunications disconnect

Most of the changes by telecommunications companies came from Global Network Initiative members.

In March 2017, **Orange**, **Telefónica**, and **Vodafone** joined the Global Network Initiative (GNI), along with four other members of the now-disbanded Telecommunications Industry Dialogue (TID).[84] As Figure 17 illustrates, over the past year those three GNI companies implemented substantial and meaningful changes to their disclosed policies affecting users' freedom of expression and privacy. Other telecommunications companies evaluated for the Index remained largely static over the past year—including AT&T, which was previously a member of the TID and held GNI observer status for one year, but did not join GNI along with its European peers.

Improvements by these companies occurred in the absence of significant legal and regulatory change, with the exception of Europe's new data protection regulations that come into force in May 2018 (hence, requirements for greater disclosure and more responsible data handling practices under these regulations, discussed in Chapter 3, were not yet fully implemented by companies when Index research ended in January 2018).[85] It appears that GNI membership was the main driver of the improvements by Orange, Telefónica, and Vodafone in the 2018 Index—and that it is a catalyst and framework for multinational telecommunications companies to improve their commitments, policies, and disclosures affecting users' freedom of expression and privacy rights, at least in relation to corporate governance and responses to government demands.

Yet the GNI framework is incomplete: it is focused primarily on increasing transparency and accountability around government demands for shutdowns, censorship, and surveillance. Commercial practices that also affect global information flows, along with commercial data protection and privacy issues, have generally fallen outside GNI's scope of work. Thus it is not surprising that the three GNI telecommunications companies made their greatest gains in the Governance category of the Index (see Chapter 3 for a full analysis of 2018 governance scores). In the Freedom of Expression and Privacy categories, improvements were found mainly in transparency reporting: specifically, improved disclosure of data and policies related to government requests to restrict information flows or requests to hand over user data.

How were telecommunications companies selected and evaluated?

The 10 telecommunications companies in the Index were selected due to their global footprints—with operations across multiple countries—and geographical diversity of their "home" countries. Added together, the operations of these multinational companies span across developing and major OECD markets. These companies own operating subsidiaries in multiple markets, and must comply with specific regulatory regimes on a country-by-country basis, but also answer to the group-level corporation. Due to resource limitations, RDR evaluated only the home country operating company of each telecommunications company group. 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.

For more about Index scoring and evaluation, see Section 1.4.

Telecommunications companies provide the fixed-line and mobile internet service necessary for users to access the platforms and services offered by internet and mobile ecosystem companies. Governments can require that such companies block users' access to blacklisted websites. Most countries block child exploitation material, while others block a broader set of content, which can include political and religious material. Some governments require telecommunications companies to block users' access to specific internet or mobile ecosystem companies' applications or websites if those companies fail to comply with content-removal demands to their satisfaction. The long-term blocking of Facebook, Twitter, and YouTube in China is just one example of this. Governments can also compel telecommunications companies to shut down all access to fixed-line or mobile internet services. (See Section 7.2 below for further discussion of network shutdowns.)

In a 2017 report, David Kaye, U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted that governments increasingly exercise power over telecommunications companies in ways that violate human rights norms by being over-broad, non-transparent, unaccountable, and lacking due process.[86] Unlike internet and mobile ecosystem companies which can serve users remotely, telecommunications companies must be present on the ground and are obliged to uphold domestic laws as well as the terms of their license agreements with the host government. These companies can also face "extra legal intimidation, such as threats to the safety of their employees and infrastructure in the event of non-compliance."[87]

Telecommunications companies in this Index are under pressure to comply with an increasing number of government demands to shut down networks or block access to websites, combined with pressure from civil society to be more accountable about when and why they do so. Laws—and regulatory ambiguity—in many countries prevent telecommunications companies from performing well in the Index. Individual company report cards identify specific ways that the law hinders each company from respecting users' rights. Yet we have also identified ways that all telecommunications companies in the Index can improve their commitment and disclosure, even under current regulatory and legal realities.

7.1. Chokepoints for global information flows ## {#section-71}

Lack of transparency by telecommunications companies makes it impossible for people to understand why, how, and under whose authority, their speech and access to information is blocked or restricted through their mobile or fixed-line internet service provider.

When a person suddenly cannot access news websites through their phone or office internet connection, who do they hold responsible? The internet service provider or their government? When a candidate for an opposition party does not know how, when, by whom, and under what authority she may be tracked and monitored through her smartphone, the implications for human rights and accountable governance in her country are serious. Yet, to varying degrees, that is the reality for users of all the telecommunications companies evaluated by the Index.

The 2018 Index includes eight indicators evaluating how transparent telecommunications companies are about policies and practices for policing content and access—both as a result of enforcement of their own private rules and as a result of compliance with external requests from governments and other third parties. We expect companies to clearly disclose what types of content and activities they prohibit (F3), and to publish data about the volume and nature of content and accounts they removed or restricted for violating these rules (F4). Companies should also clearly disclose policies for responding to government and private requests to restrict content and user accounts (F5), and publish data about the types of such requests they received and with which they complied (F6, F7). We expect companies to disclose that they notify users when they have removed content, restricted a user's account, or otherwise restricted access to content or a service (F8).

Results of the 2018 Index show that these companies reveal little about their content-blocking activities—whether as a result of enforcing their own rules, or demands from governments and other external entities to block websites or shut down networks (Figure 18).

As Figure 18 shows, there were few improvements. **Telefónica** demonstrated the most improvements of any telecommunications company, clarifying reasons it may not comply with government requests (F5), and disclosing more detail about the number of government requests that it received to restrict content or accounts that it received and the number of those requests with which it complied (F6). The company, along with **AT&T**, **Orange**, and **Vodafone**, also improved disclosure of its handling of government demands to shut down networks (F10).

Disappointingly, **Axiata** and **Vodafone** were less transparent than in the 2017 Index about whether they have policies of notifying users when they block content or restrict a user's account (F8). Vodafone's most recent Law Enforcement Disclosure report,[88] which outlines the company's approach to handling content restriction requests from governments and law enforcement, did not specify whether it notifies users who attempt to access content that it has been restricted, whereas the previous version of this report did.

No company improved disclosure about its network management policies and practices (F9). Bharti Airtel's score even declined on that indicator (see company report card in Chapter 10 for details).

7.2. Network shutdowns ## {#section-72}

Despite small improvements, a lack of disclosure from companies on network shutdown policies leaves users in the dark about this human rights threat.

Network shutdowns pose a threat to human rights. When telecommunications companies cut off access to their networks, millions of people can be left without the ability to communicate. This threat is particularly acute during times of political crisis, when the ability to communicate is most vital and when authoritarian governments more often impose such restrictions. In June 2016, the United Nations Human Rights Council adopted a resolution condemning network shutdowns and other intentional restrictions on access as violations of international human rights law.[89]

According to the global advocacy group Access Now there were more than 116 network shutdowns documented around the world between January 2016 and September 2017.[90] The Software Freedom Law Center documented 70 shutdowns in 2017 in India alone.[91] The issue has received global attention thanks to persistent civil society campaigning, including a multi-year campaign by Access Now. The Global Network Initiative (GNI) has committed to conduct policy advocacy to end the practice,[92] and the governmental Freedom Online Coalition has declared network shutdowns to be a violation of human rights.[93]

While telecommunications companies cannot stop governments from demanding shutdowns and threatening their staff, the Index rewards those that disclose their policies and practices for responding to government shutdown demands. Ideally companies should also report data about the volume and nature of shutdown orders received, and the number complied with.

There is a long way to go: the average score on this indicator was just 18.75 percent, with all companies failing to provide sufficient information about how they respond to such demands.[94] While four telecommunications companies—**AT&T**, **Orange**, **Telefónica**, and **Vodafone**—improved their disclosure of how they deal with government requests to shut down networks, all companies still lacked transparency.

An examination of company disclosure reveals the following:

- **Telefónica** and **Vodafone**, both Global Network Initiative (GNI) members, disclosed more than the rest of their peers about policies and practices for handling network shutdown orders by authorities.

- **Telefónica** was the only company to disclose the number of shutdown orders it received and to clearly list the legal authority in each country from which it received shutdown orders. The company also clarified why it may push back against, or reject, a network shutdown demand and provided some data about its compliance with these types of orders. It disclosed information on the circumstances under which it would restrict access to its service or restrict certain types of traffic, although its disclosure was not as comprehensive as Vodafone’s.

- **Vodafone** was the only company to clearly disclose its process for responding to these types of government demands and to clearly commit to push back against demands when possible. The company also disclosed clear policies about the circumstances under which it would restrict access to its service or restrict certain types of traffic and clarified how the company weighs the the freedom of expression risks associated with these types of requests.

- While only **Telefónica** disclosed the number of shutdown requests it received, **AT&T** improved its disclosure in this regard by stating that it would disclose the number of shutdown requests it received if it had received any.

- **Orange** improved its disclosure by detailing an example from 2011 in which it pushed back on a shutdown request from the Egyptian authorities.

Several companies had particularly low levels of disclosure, and made no improvements since the 2017 Index, including **Bharti Airtel**, **Axiata**, **Ooredoo**, and **América Móvil**.

- **Bharti Airtel** disclosed almost nothing about how it responds to government requests to shut down its networks, aside from very broad language about reasons why service might be disrupted. While Indian law prevents companies from disclosing information about specific government shutdown orders,[95] there is no legal obstacle to disclosing clear reasons why the company may have to shut down its networks or company policies for evaluating and responding to shutdown requests, and there is also no obstacle to having a policy to notify users about shutdowns.

- **Axiata** and **Ooredoo** also disclosed only very broad or vague reasons why their service might be disrupted. Neither company's home jurisdiction has laws restricting disclosure of the company's process for responding to these types of requests. Both companies could be more transparent about how they respond to shutdown requests, the reasons why shutdowns might occur, and whether they have a policy of notifying users about shutdowns.

- **América Móvil** disclosed no information whatsoever about its handling of network shutdown requests, even though no laws in Mexico bar such disclosure.

7.3. Policing access to information ## {#section-73}

Telecommunications companies disclose almost nothing about how they handle or comply with government and private requests to block content or user accounts.

Just four companies—**AT&T**, **Etisalat**, **Telefónica**, and **Vodafone**—disclosed anything about their process for handling government requests to block content (Figure 20). Only two companies—**AT&T** and **Telefónica**—supplied data about such requests.

Vodafone disclosed more than its peers about its process for handling third-party requests, but then disclosed no data about its compliance with these requests. No telecommunications company provided any data about private requests it received to restrict content or accounts.

While most telecommunications companies disclosed some information about what types of content or activities are prohibited on their services, none disclosed any information about what actions they take to enforce these terms.

Telecommunications companies have the ability to block content or access to their services, according to their own internal rules and in line with the regulations of the country in which they operate.

Most telecommunications companies provide some information about their rules in their terms of service, however, Index results show that most companies failed to provide enough information about these rules in order for users to understand what actions companies take to enforce them (Figure 21). As gatekeepers to the internet, these companies should be more transparent about the role they play in policing users' access to information.

No telecommunications company made any improvement on indicators related to terms of service enforcement in the 2018 Index. None published any data about the volume of content or URLs it blocks or user accounts it otherwise restricts or suspends, as a result of breaches to those terms.

While every telecommunications company in the Index disclosed some information about the policies for enforcing its terms of service, disclosure is inadequate across the board, with some companies disclosing very little. As Figure 21 shows, **Orange France** disclosed more than any other telecommunications company, followed by **Telefónica Spain**, **AT&T**, and **Vodafone UK**.

Results also show:

- Six out of the 10 telecommunications companies—**Telcel (América Móvil)**, **Etisalat UAE**, **Ooredoo Qatar**, **Orange France**, **Telefónica Spain**, and **Vodafone UK**—received full credit for their disclosure of what types of content or activities they prohibit, and the reasons why they may restrict a user's account. **AT&T** also earned high scores on these elements but fell short of comprehensive disclosure for its post-paid mobile service.

- **Telcel (América Móvil)**, **AT&T**, **Etisalat UAE**, **Orange France**, **Telefónica Spain**, and **Vodafone UK** each disclosed at least some information about its process for enforcing its rules, including steps it may take when a user violates its terms.

- **AT&T**, **Telefónica Spain**, and **Vodafone UK** provided some information about how they identify content or activities that violates their rules, though none fully disclosed how they identify these breaches.

- The lowest scoring companies—**Celcom (Axiata)**, **Airtel India (Bharti Airtel)**, **Ooredoo Qatar**, and **MTN South Africa**—disclosed no information other than the types of content or activities they prohibit and why they may restrict a user's account.

7.4. Privacy problems: surveillance and data protection ## {#section-74}

Users don't know much about who has access to their information, for what purposes, under whose authority, and under what circumstances.

As providers of fixed-line and mobile data services, telecommunications companies know what websites and applications people access. They have direct access to all of their users' unencrypted communications. All of this information can be shared with governments, commercial partners, and other third parties.

Without transparency about what information is collected, how long it is retained, what is shared with whom, and for what purposes and under whose authority, there is neither accountability nor basic checks against abuse. If people's information is used for surveillance purposes that violate basic international human rights norms, they cannot to hold their abusers accountable. If personal information is shared without users' knowledge and consent with parties who use it for commercial purposes, it is difficult to identify perpetrators and obtain redress when the user falls victim to predatory or discriminatory economic, financial, social, or political targeting.

While there are legitimate national security and law enforcement reasons why users should not be notified in real time when their information is shared with authorities, people have a right to know the circumstances under which they can expect their information to be shared, and with whom. People have a right to know that companies have rigorous policies in place to prevent access to personal data that is not requested lawfully. Furthermore, there are no legitimate public interest reasons why companies should not be transparent about the sharing of information with commercial and non-governmental parties.

Given the amount of sensitive information telecommunications providers may have access to about people who use their services, it is reasonable to expect companies to publish the privacy policies that govern how they handle this information. Users should be able to assess and compare the privacy policies of different companies and services *before* they make a choice to subscribe and hand over their user information, and other interested parties, like investors, should be able to evaluate a company's data handling policies in order to gauge potential risks. Companies should also publicly commit to notify users of any changes to their privacy policy and to make these changes public, so that users are fully aware of any shifts in how a company collects, shares, uses, or retains their information.

Our researchers did not identify any legal or regulatory reasons why all of the telecommunications companies in the Index should not earn full credit for publicly disclosing clear and accessible privacy policies, and for notifying users of changes to those policies. Yet as Figure 22 shows, even such basic disclosure is a challenge for many.

The privacy policies for **Telcel (América Móvil)**, **Celcom (Axiata)**, and **Telefónica Spain** were easy to find and available in the primary languages of their home markets, but these policies were not presented in a way that would be easy for most consumers to understand. The privacy policy for **Airtel India (Bharti Airtel)** was easy to find, but was not available in languages other than English and was divided across several separate documents, making it difficult for users to comprehend the scope of the terms. **MTN South Africa's** privacy policy was presented in a more easily read manner than Bharti Airtel's, but was not as straightforward to find on the company's website, and was not available in the primary languages (other than English) of MTN's home market.

AT&T was the only telecommunications company to commit to notify users of changes to its privacy policy. It provided users with a timeframe for notice, but failed to disclose that it would directly notify users of these changes, instead opting to post them on its website, which is not considered a form of direct notification.

Etisalat UAE and **Ooredoo Qatar** were the only two telecommunications companies for which researchers were unable to locate a publicly available privacy policy for their services.

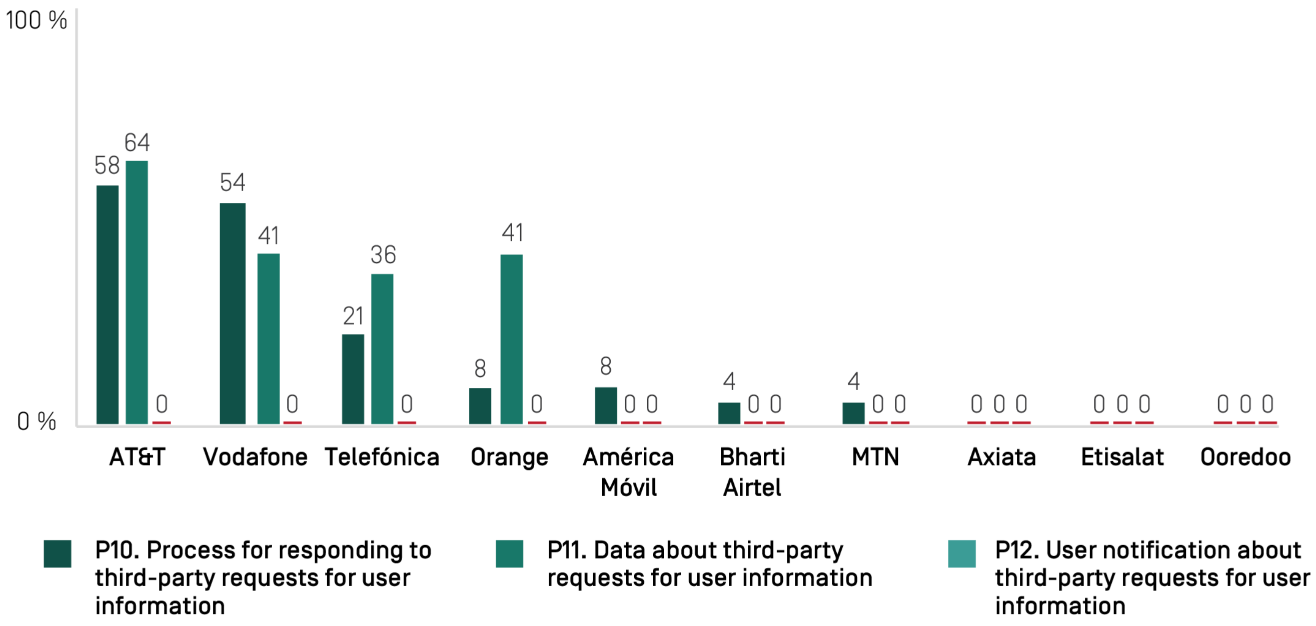
Opacity in the Arab region The absence of publicly disclosed privacy policies by Etisalat UAE and Ooredoo Qatar is an example of how telecommunications companies lack transparency across the Arab region. Research by Social Media Exchange (SMEX), a Beirut-based media development and digital rights organization, found that of the region's 66 mobile operators, only seven published privacy policies. Of these seven companies, two are subsidiaries of the Vodafone group, a GNI member: Vodafone Egypt and Vodafone Qatar. None of the five subsidiaries of Orange, also a GNI member, published privacy policies. These subsidiaries are Orange Egypt, Orange Jordan, Orange Morocco, Orange Tunisia, and a joint venture company Korek Telecom (Iraq). There are no apparent legal factors preventing Orange from publishing its privacy policies in these countries. For example, the SMEX report found that other operators in Tunisia and Jordan, LycaMobile Tunisia and Zain Jordan, published privacy policies. **Read more at:** "Dependent Yet Disenfranchised: The Policy Void That Threatens the Rights of Mobile Users in Arab States," The Social Media Exchange (SMEX), January 2018, https://smex.org/dependent-yet-disenfranchised-the-policy-void-that-threatens-the-rights-of-mobile-users-in-arab-states/.

Surveillance accountability: Companies fail to provide maximum, legally permissible transparency about how they handle third-party requests for user information.

Many countries have over-broad surveillance laws that do not require basic transparency and accountability on the part of government authorities. These laws also often prevent telecommunications companies from disclosing even general information about the companies' processes for complying with demands and what information is shared with authorities. Thus, some companies have their home governments—and laws that breach international human rights standards—to blame for their lack of transparency regarding how they handle government requests for user information. Nonetheless, there are ways that each and every one of the telecommunications companies in this Index can improve their scores on these indicators.

Index data shows that of the 10 telecommunications companies evaluated, seven disclosed some information about their process for evaluating and responding to requests to hand over user information—and only four of these companies provided any data on the number of such requests they received, or the number with which they complied (Figure 23).

Figure 23 | How transparent are telecommunications companies about government and private requests for user information [P10, P11, P12]?



Results revealed the following:

- **Orange** and **Telefónica** both improved their disclosure of how they handle government requests for user information. Orange disclosed data about the number of requests it received from French authorities for real-time and stored communications data. Telefónica disclosed some data about the number of accounts affected by government requests and its compliance rates.

- Three companies—**Axiata** (Malaysia), **Ooredoo** (Qatar), and **Etisalat** (UAE)—disclosed no information whatsoever about their processes for responding to government and private requests for user information. Yet all three of these companies could make significant improvements to their disclosure without changes to the laws in their home jurisdictions. In Qatar and the UAE, telecommunications companies may be required to give government officials direct access to their networks, so while they may not have precise data about the number of times government officials accessed user information, there is nothing in the law preventing Ooredoo and Etisalat from disclosing information about these processes.[96] And while Malaysia's Official Secrets Act may prohibit some disclosure of government requests, nothing prevents Axiata from publishing at least some information about how it handles third-party requests for user information.[97]

- The highest-performing companies—**AT&T** and **Vodafone**—each disclosed clear information about how they respond to judicial and non-judicial government requests and requests from foreign jurisdictions, the legal basis under which they comply with such requests, and a commitment to conduct due diligence and push back against overbroad government requests. However, neither company disclosed information about their processes for responding to private requests, or data about such requests that they received, even though there are no specific legal barriers preventing them from doing so.

- **América Móvil** and **Bharti Airtel** disclosed very minimal information about their processes for responding to requests for user information. There are no legal barriers in Mexico preventing América Móvil from disclosing information about how it evaluates and responds to such requests. Indian law prevents companies like Bharti Airtel from publishing data on government requests for user information but does not prevent them from disclosing their processes for responding to these requests.

No telecommunications company disclosed information about their policies for notifying users when their information is requested. While laws may prohibit companies from notifying users when a government official demands a user's information, most companies could still at least disclose the situations in which they are prohibited from notifying users, and their notification policies for private requests.

Data protection: Telecommunications companies fail to disclose clear information about collection, use, and sharing of personal information

The 2018 Index includes six indicators evaluating corporate transparency about handling of user information.[98] We expect companies to disclose what information they collect (P3), what information they share and the types and names of the third parties with whom they share it (P4), the purpose for collecting and sharing user information (P5), and for how long this information is retained (P6). Companies should also provide clear options for users to control what information is collected and shared, including for the purposes of targeted advertising (P7). We expect companies to clearly disclose how users can obtain all public-facing and internal data they hold on users, including metadata (P8).

Results of the 2018 Index show that telecommunications companies were generally less transparent than internet and mobile ecosystem companies about their handling of user information, including what data they collect, share and for what purpose, whether users have any control over what is shared, and whether users can obtain all the information a company holds on them.

As in the 2017 Index, **AT&T** disclosed more than any other telecommunication company, including the three European companies (Orange, Telefónica, and Vodafone) about its handling of user information (Figure 24).

There was little improvement across these indicators for the 2018 Index: two companies—**AT&T** and **Orange**—improved disclosure of options users have to access their information (although none disclosed that users can access all of the information a company holds on them). Telecommunications companies disclosed particularly little about data retention policies: only two companies, **AT&T** and **Vodafone**, disclosed any information, and what they did disclose is scant.

While **AT&T** disclosed little regarding its handling of user information, it performed better on this set of indicators than all of the other telecommunications companies evaluated in the Index. The company was slightly more transparent about what user information it collects, as compared to what it shares, and the purposes for doing so. AT&T provided little information on how long it retains user information, but was the only company other than Vodafone to provide any relevant information.

It is notable that, even with Europe's strong data protection laws, EU-based telecommunications companies had insufficient and inconsistent disclosure of how they collect, share, retain, and otherwise handle user information, particularly next to their U.S. peer, AT&T. While these companies may be communicating with regulators about data collection, handling, and sharing to ensure compliance with the law, as of January 2018 when research for this Index was concluded, these companies were still not communicating clearly with the public. As Europe's new privacy regulations come into force in the middle of 2018 we hope to see further improvement in European companies' disclosure about how they handle user information.

Several jurisdictions lack adequate data protection laws, and companies headquartered in these jurisdictions tend to disclose no more than the law requires, resulting in low Index scores. In the UAE, where **Etisalat** is headquartered, there is no data protection law or general privacy law. In other places the law provides wide loopholes: in Qatar, where **Ooredoo** is headquartered, companies are exempt from complying with the data protection law if they are executing a court order, collecting information pertaining to a crime per police request, or other exceptions. (As noted previously in this chapter, privacy policies of Etisalat and Ooredoo are not made publicly available.) In South Africa, where **MTN** is headquartered, the company's low privacy score appears related to the fact that the Protection of Personal Information Act (POPI) still has not yet entered into force, even though it was signed into law in 2013.[99] In India, the Supreme Court's 2017 ruling that privacy is a fundamental constitutional right has become the basis for development of a new data protection law that has potential to drive improved disclosure by Indian ICT-sector companies, including **Bharti Airtel**, in the near future.

7.5. Recommendations for telecommunications companies ## {#section-75}

- **Work with civil society and legislators to enact legal reforms aimed at ensuring that the law enables maximum respect for users' privacy rights.** In particular, companies should use every opportunity available to encourage governments to move away from mass surveillance and institute meaningful oversight over national security and law enforcement authorities, in accordance with The International Principles on the Application of Human Rights to Communications Surveillance.[100]

- **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).

- **Commit to push back against network shutdown requests, and disclose data regarding the number of such requests received.** Network shutdowns continue to threaten users' ability to exercise their rights. Given these growing threats, companies must endeavor to disclose as much information as possible about their processes and principles for responding to such requests, and confirm the number of requests they received.

- **Publish comprehensive transparency reports.** Companies should publish regular information and data on their official websites that helps users and other stakeholders understand the circumstances under which personal information may be accessed, or when access to service may be blocked or restricted. Such disclosures should include 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.

- **Disclose meaningful data about government requests to restrict content or accounts.** While some companies disclose some data about these requests, more disclosure is needed. In particular, companies should disclose the number of requests they receive per country as well as the number of requests with which they comply.

- **Clarify private processes through which websites may be blocked or accounts may be restricted.** Compared to their disclosure about government requests, companies disclose less about how they respond to private requests to restrict content or accounts, and what types of private requests they will consider. Companies should therefore improve their disclosure by clarifying under what circumstances they will respond, and by confirming that they conduct due diligence on such requests.

- **Commit to notifying users of censorship events.** Companies should disclose their policies for notifying users when they restrict their content or accounts, including the reason for doing so.

- **Disclose meaningful data about terms of service enforcement.** Companies should issue transparency reports, ideally every six months, showing the number of actions they took to remove content or restrict accounts that violated their rules, and the reasons for doing so (e.g. the number of accounts restricted for posting extremist content, the number of items removed for containing hate speech, etc).

- **Provide examples of how rules are enforced.** Even when companies publish their rules, it is very unclear how they are enforced. Reports of arbitrary blocking or inconsistent restrictions on accounts make it all the more difficult to understand how platforms are being policed. Clearer disclosure on this front will help restore trust between users and the services on which they rely, and could help empower users to understand and seek remedy when their content or accounts have been unfairly restricted.