RANKING DIGITAL RIGHTS

2018 CORPORATE ACCOUNTABILITY INDEX

The Ranking Digital Rights 2018 Corporate Accountability Index evaluates 22 of the world's most powerful internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy.

RANKINGDIGITALRIGHTS.ORG/INDEX2018

APRIL 2018

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 New America's 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, 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, 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'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.

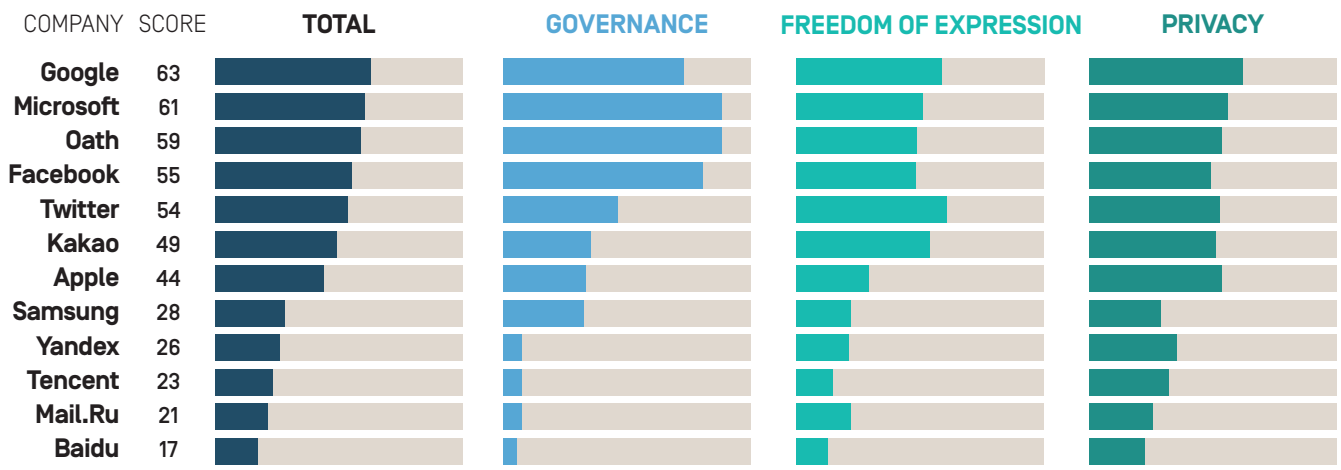
Contents

Contents, cont.

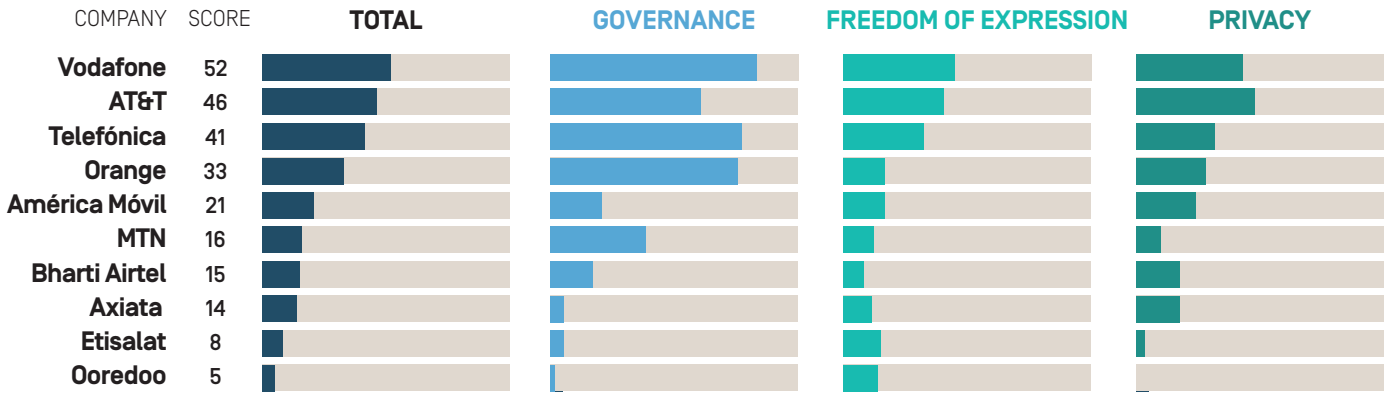
Contents, cont.

2018 Corporate Accountability Index

● INTERNET AND MOBILE ECOSYSTEM COMPANIES



● TELECOMMUNICATIONS COMPANIES



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 people 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, communities, and individuals.

- **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. To view in-depth results and data visualizations, download full datasets, and access related resources, news, and updates, please visit: https://rankingdigitalrights.org/index2018.

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 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, 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.

> **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.**

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.

I. 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 affecting 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, Daum Mail, 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

Research for the 2018 Index was based on company policies that were active between January 13, 2017 and January 12, 2018.

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.[17]

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 by 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. Some 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. Such 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 visit the 2018 Index website at: https://rankingdigitalrights.org/index2018. 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.

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.

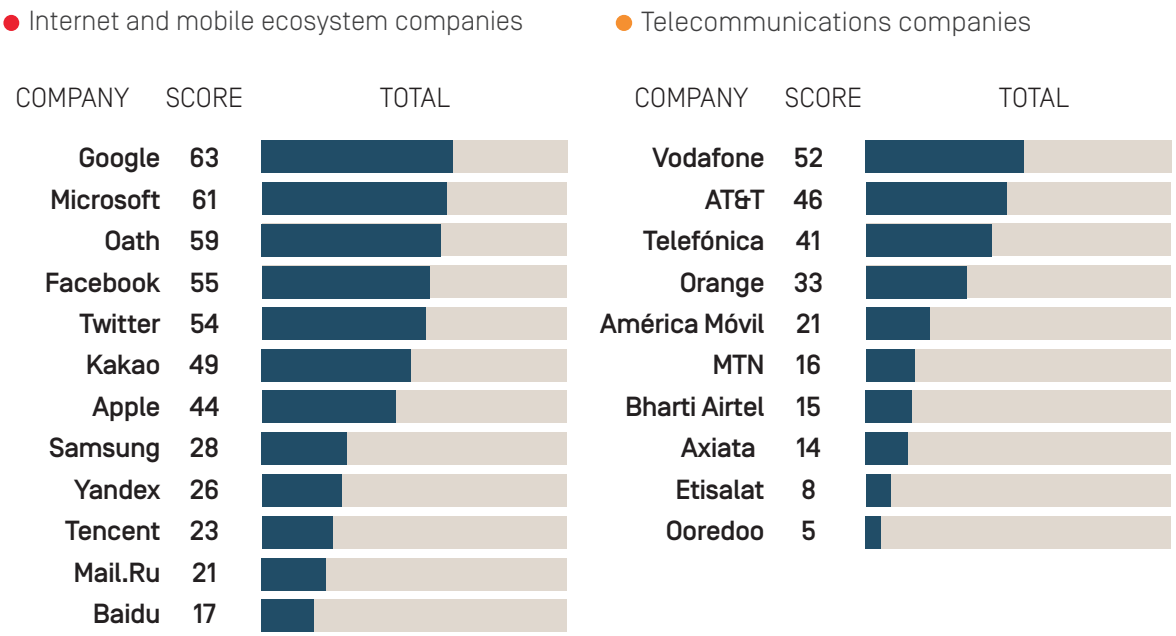
4. **Expression: Companies keep the public in the dark about how content and information flows are policed and shaped through their platforms and services.** Despite revelations that the world's most powerful social media platforms have been used to spread disinformation and manipulate political outcomes 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. 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

Figure 1 | The 2018 Corporate Accountability Index ranking



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, 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.

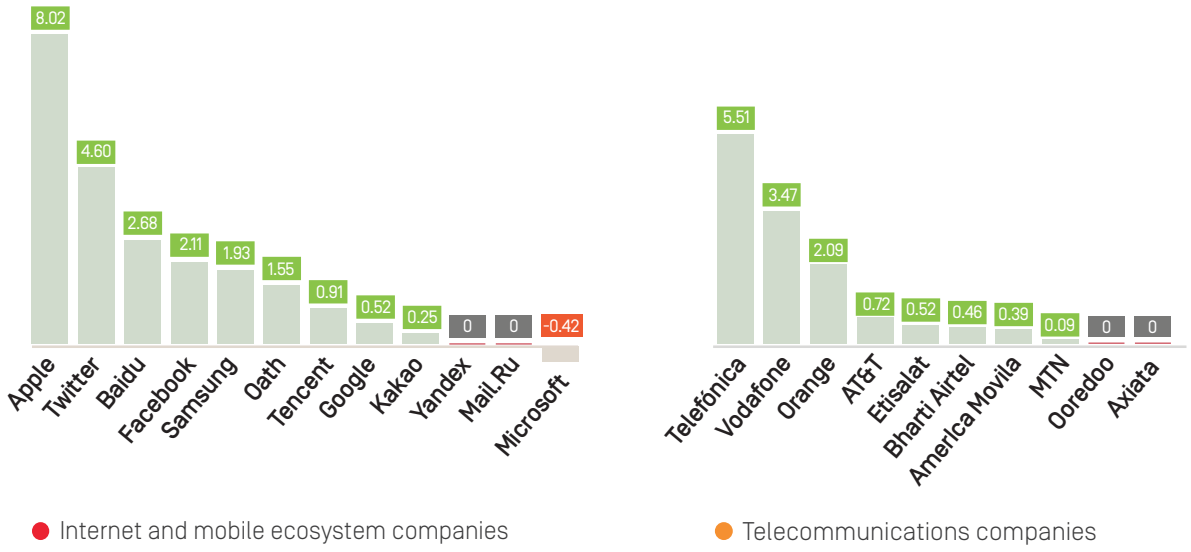
See each company's individual "report card" in Chapter 10 of this report.

3.2 Notable changes

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.

Figure 2 | Year-on-year score changes (2017 to 2018)



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.

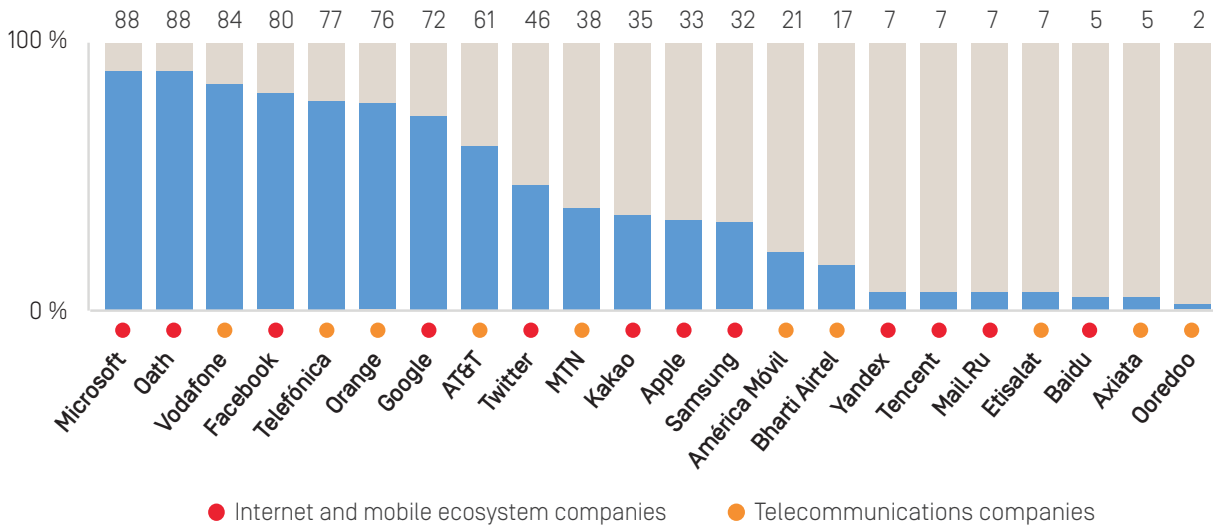
3.3 Governance advances and gaps

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.

Figure 3 | Governance scores



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.

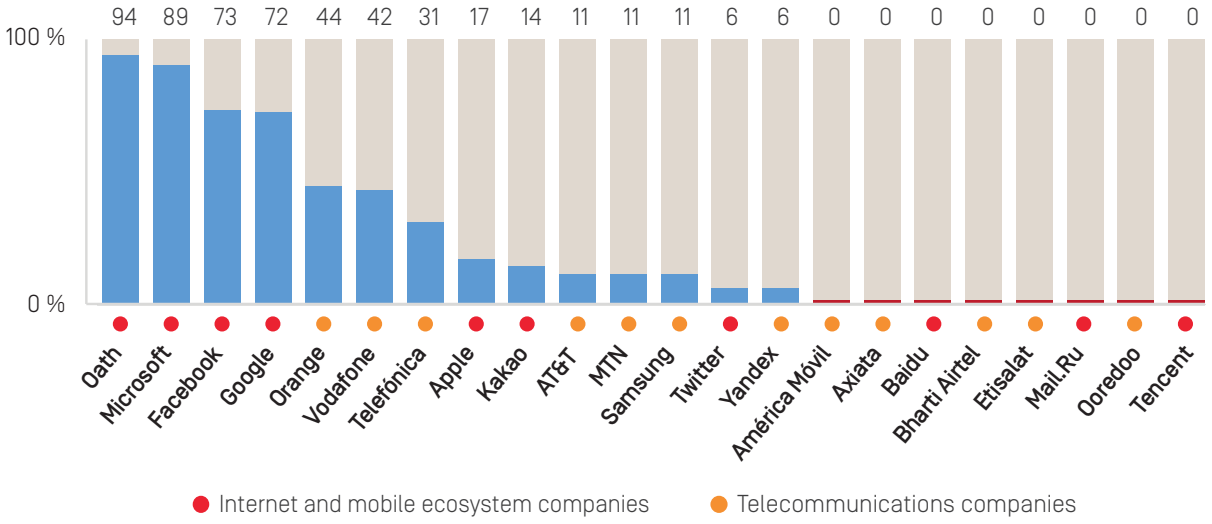
AT&T was the only non-GNI company with a governance score of more than 50 percent. However, the company's score in this category declined due to its weakened commitment to engaging with stakeholders on digital rights issues as a result of its decision not to join GNI along with its European peers and 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.

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

3.4 Spotlight: Human rights impact assessments

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.

Figure 4 | Comprehensiveness of human rights impact assessments (G4)



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 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.

Companies should be proactive in conducting human rights risk assessments to identify and mitigate how their products and services cause human rights harms.

3.5 Regulatory factors

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 on to 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

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.

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.

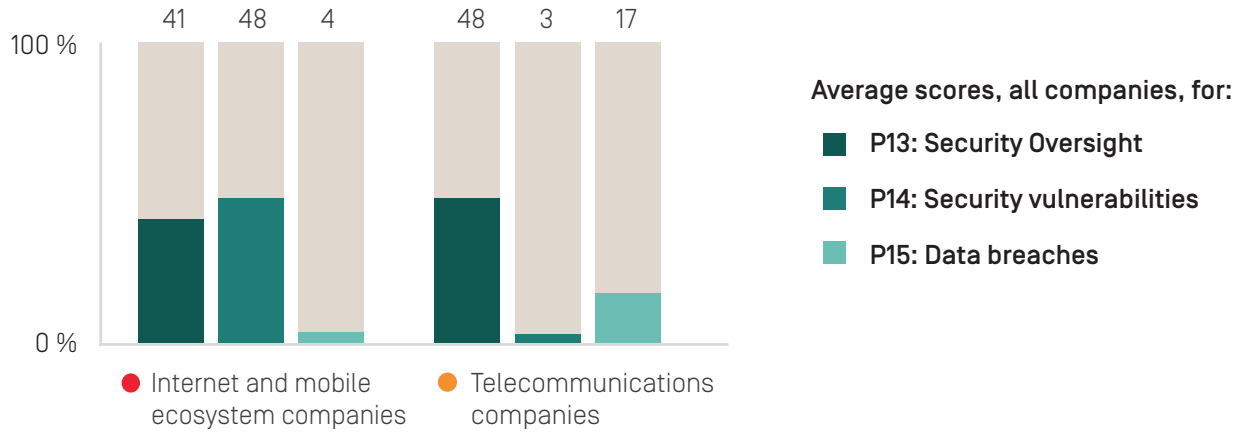
4.1 Disclosure failure

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).

Figure 5 | How transparent are companies about their internal security measures (P13-P15)?



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

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.

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.

Communicating about data breaches: What do we expect companies to disclose?

Indicator P15 contains three elements evaluating company disclosure of policies for responding to data breaches should they occur.

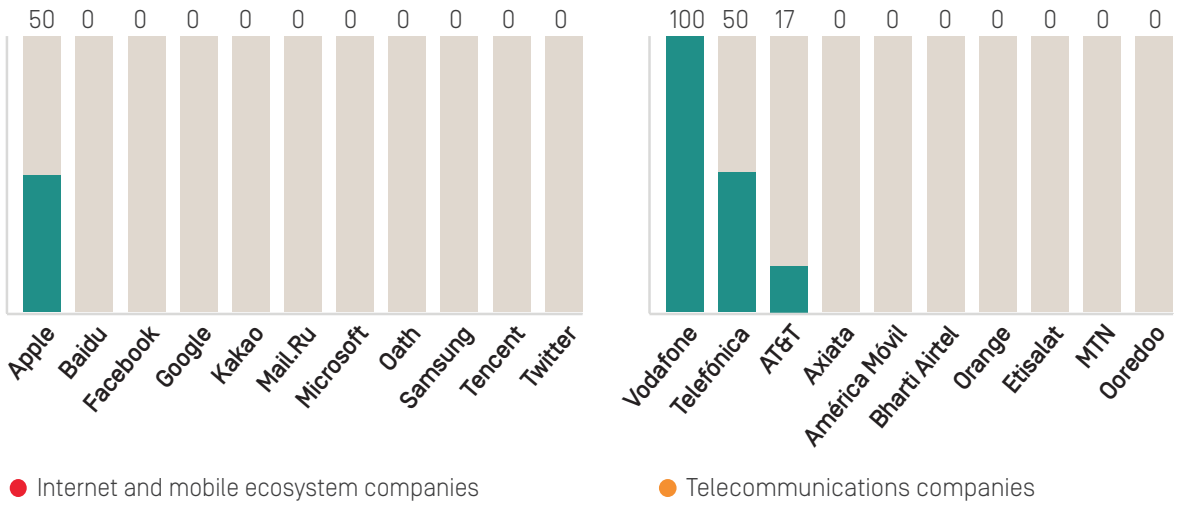
- **Element 1: Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?** Legally, companies are often required to notify the relevant authorities when a data breach occurs. This element does not focus on whether companies disclose 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.

Figure 6 | How transparent are companies about policies for responding to data breaches (P15)?



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

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.

Figure 7 | How transparent are companies about their security oversight processes (P13)?

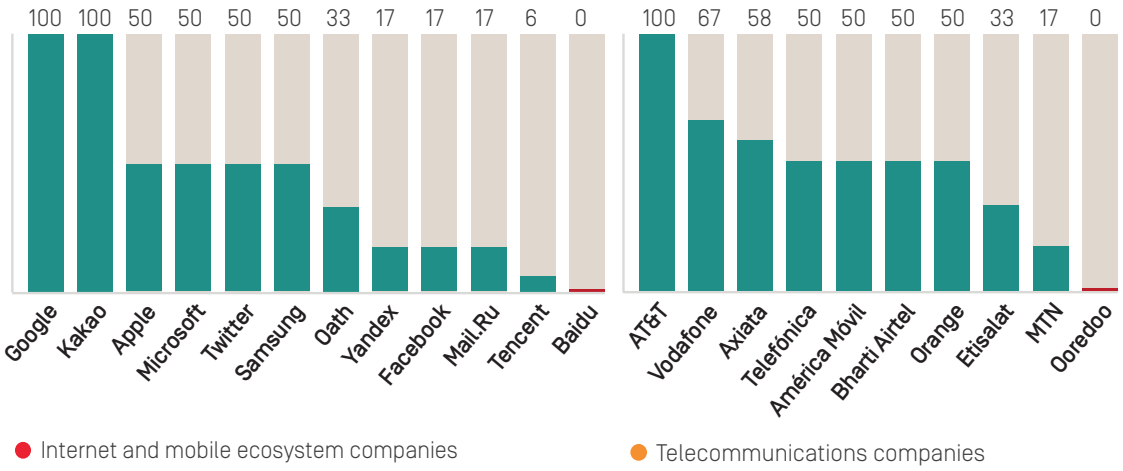


Figure 7 illustrates a wide range in companies' disclosure about security oversight processes. Notably:

- 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

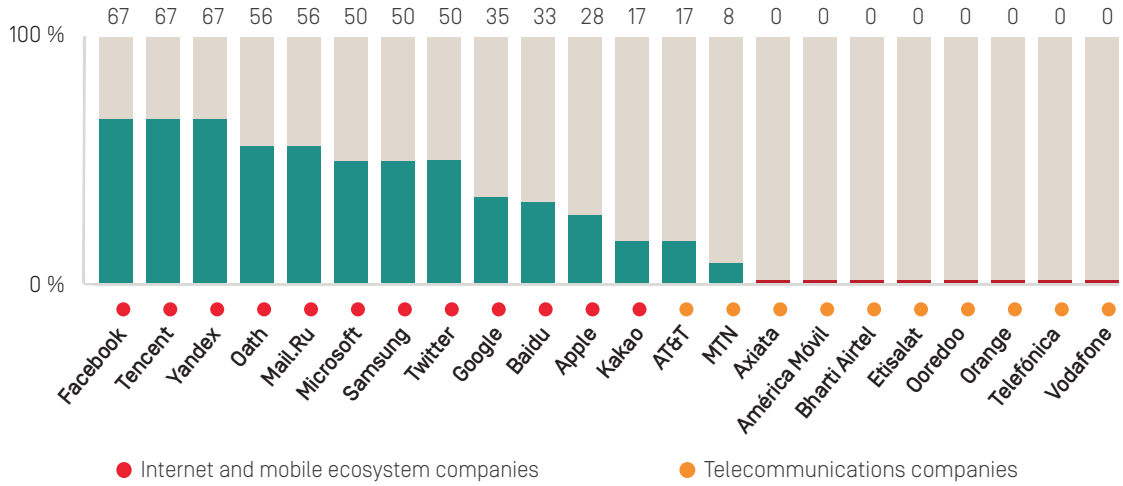
Companies lacked adequate information about how they address security vulnerabilities when they are discovered.

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.

Figure 8 | How transparent are companies about their policies for addressing security vulnerabilities (P14)?



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

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

- **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.

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).

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.

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.

Detailed user profiles can be used by governments to identify surveillance targets, or by political organizations to target individuals with tailored campaigns.

5.1 Transparency remains inadequate

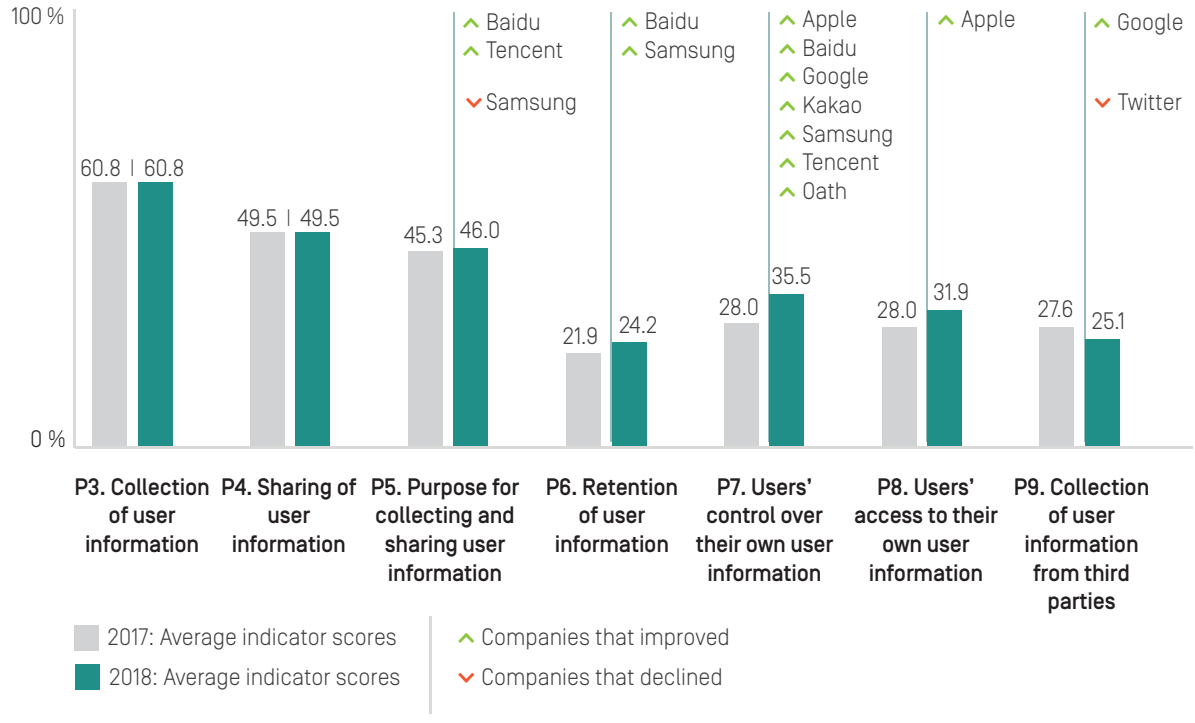
Internet and mobile ecosystem companies have made little progress in disclosing how they handle user information, and what options people have to control what is collected and shared.

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

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



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).

- 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).

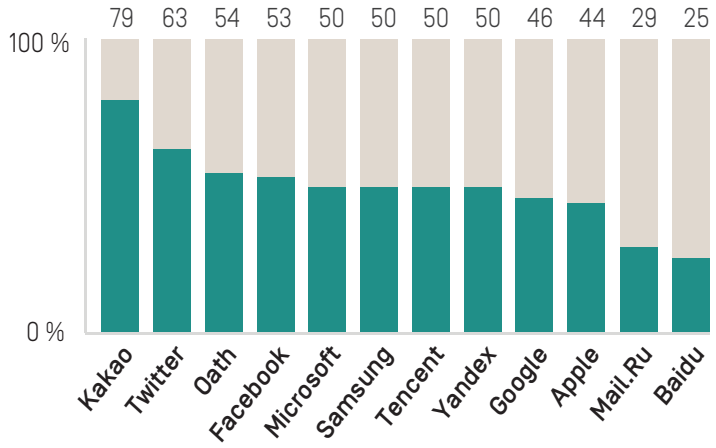
5.2 What, whom, and why?

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 information they share and with whom (P4)?

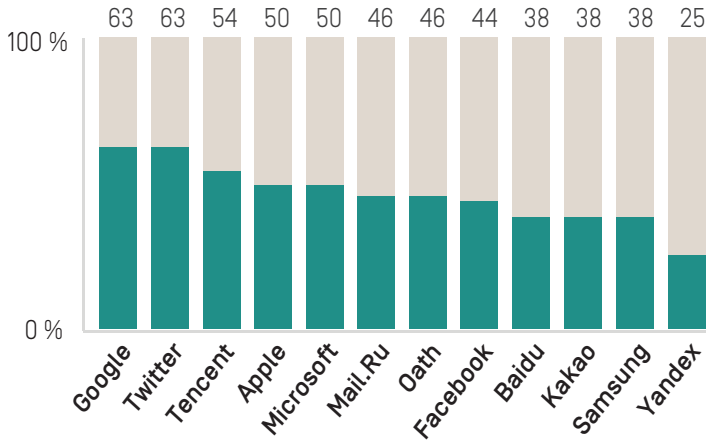


Indicator P4 evaluates company disclosure of what user information they share, including the types and names of third-parties with whom they share it. See: https://rankingdigitalrights.org/index2018/indicators/p4

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/index2018/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.

5.3 Targeted advertising and lack of user control

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.

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.

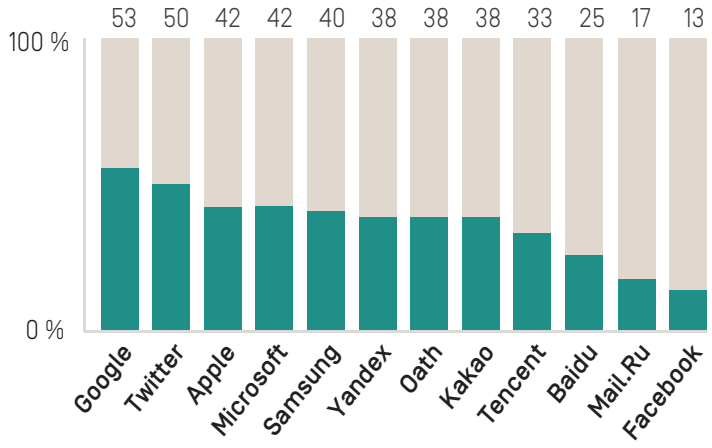
- Seven companies—**Apple**, **Baidu**, **Google**, **Kakao**, **Samsung**, **Tencent**, and **Oath**—improved their disclosure of options users have to control their information, which includes options to control if and how their data is collected for targeted advertising (P7) (see company report cards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

Despite significant public concerns regarding the invasive nature 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 said that targeted advertising was *off*—or opt-in—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, see Dipayan Ghosh 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/.

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 said that targeted advertising was *off*—or opt-in—by default.

5.4 Tracking users

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.

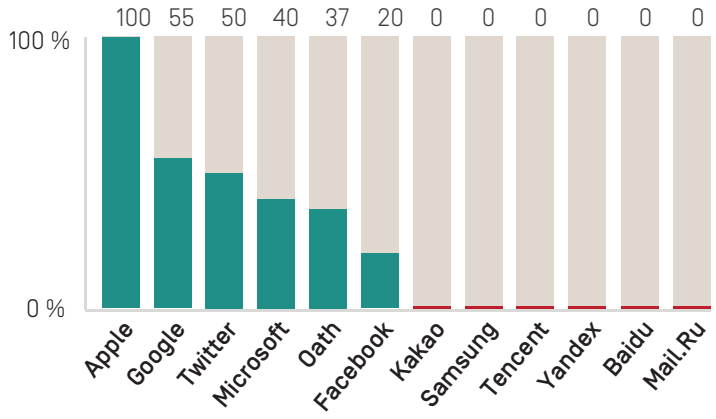
For these reasons, we expect companies to disclose that users can control geolocation data tracking. Users should be able to control geolocational data tracking at the device level, as well as on an app-by-app basis. This enables them to determine whether device manufacturers and individual applications 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 13 | How transparent are internet and mobile ecosystem companies about tracking users across the internet (P9)?



Indicator P9 evaluates company disclosure of if, how, and why internet and mobile ecosystem companies track users on third-party websites using tracking tools like cookies or widgets. See: https://rankingdigitalrights.org/index-2018/indicators/p9

- **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

- **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 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.

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.

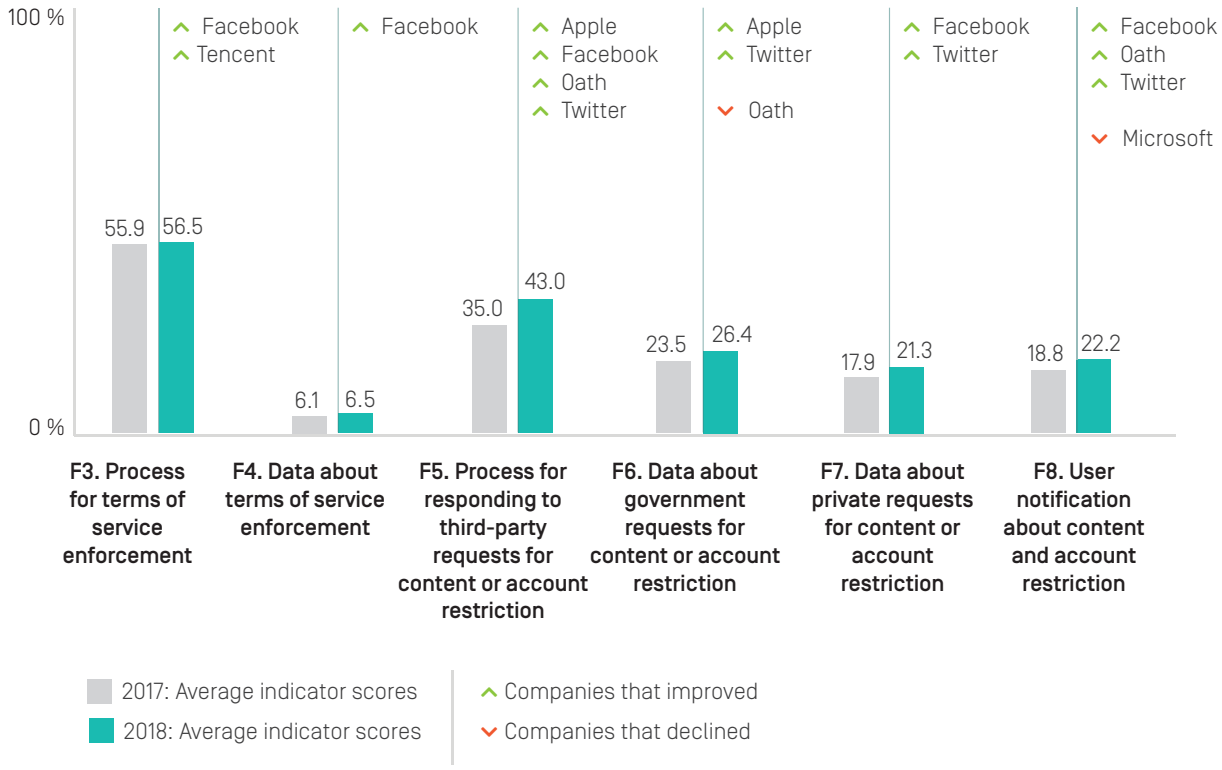
The 2018 Index therefore includes six indicators measuring corporate transparency about processes for censoring online content or restricting access to their platforms or services. Collectively, these indicators evaluate company disclosure of policies and mechanisms for compliance with government requests, 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

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]

Figure 14 | How transparent are internet and mobile ecosystem companies about policing content (F3-F8)?



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

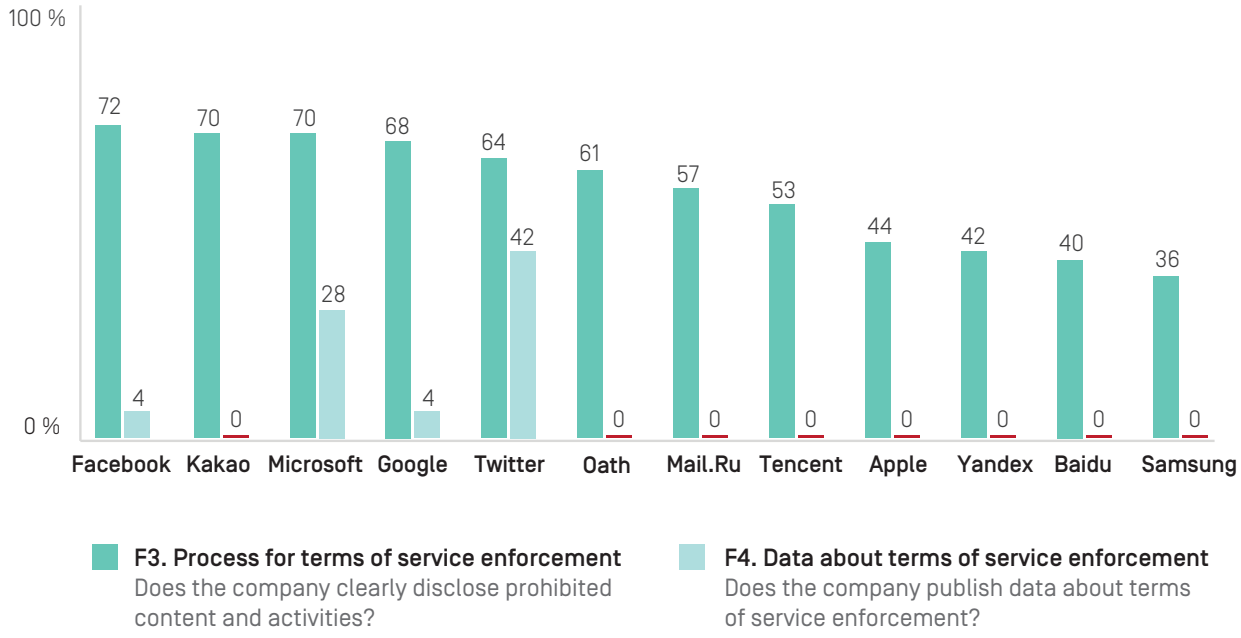
Internet and mobile ecosystem companies lack transparency about what their rules are and actions they take to enforce them.

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).

> **People have a right to know how and why their speech or access to information may be restricted or otherwise policed.**

Figure 15 | How transparent are internet and mobile ecosystem companies about their rules and how they are enforced (F3, F4)?



- **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.[65] 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 (Google) 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 organizations who will help flag content."[76] In 2017, Indonesian media reported that YouTube (Google) 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 (Google)** 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

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

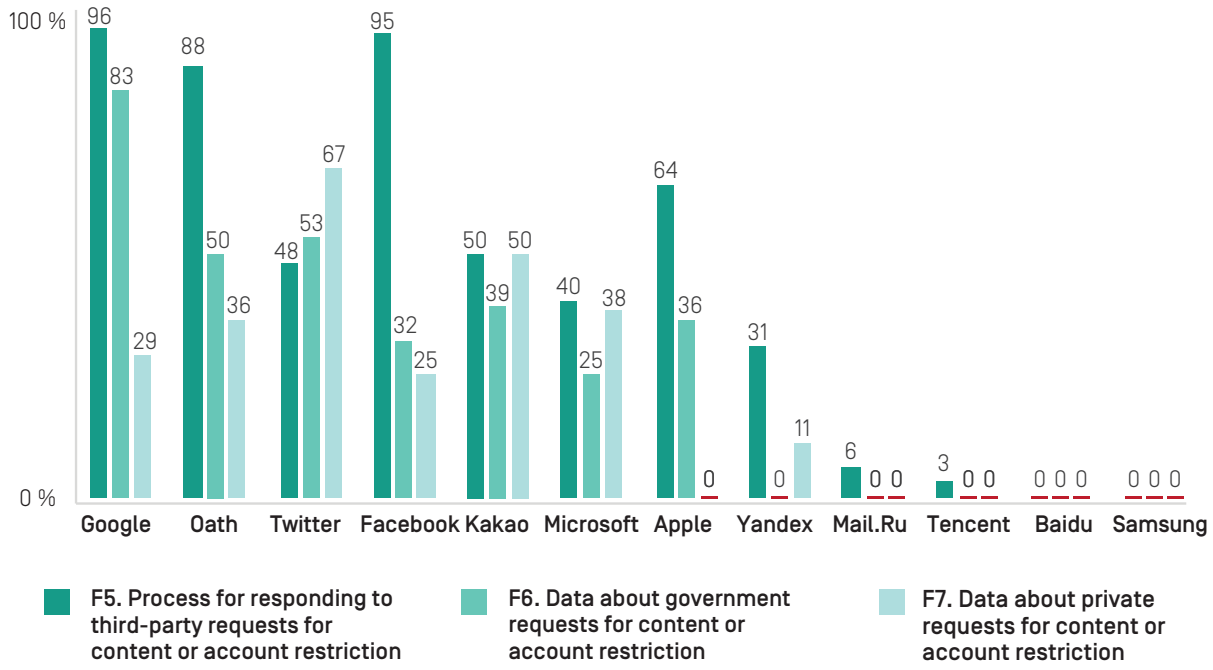
Aside from platforms' private mechanisms for flagging terms of service violations, internet and mobile ecosystem companies receive a growing number of external requests to remove content or restrict user accounts via more formal and official channels. These requests come from government agencies, law 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]

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).

Figure 16 | How transparent are internet and mobile ecosystem companies about handling external demands to censor content and restrict user accounts (F5-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.

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.

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.

6.4 Recommendations for companies

- **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.

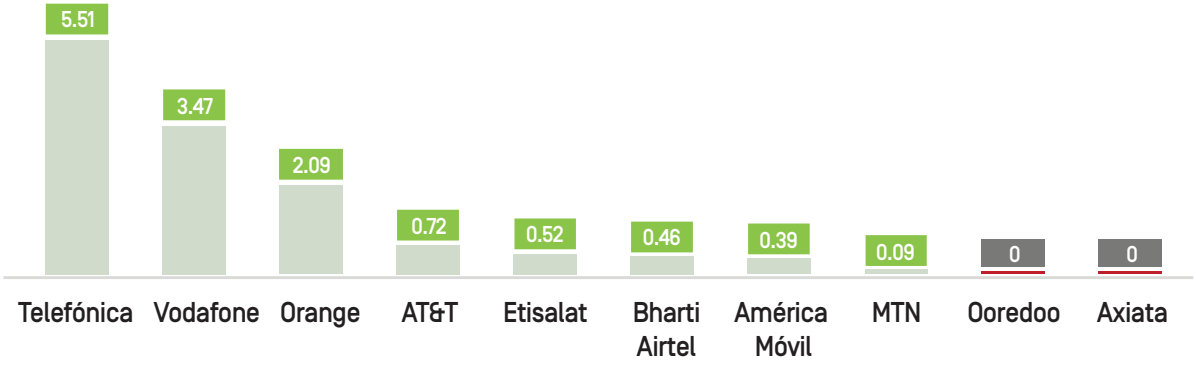
7. Telecommunications disconnect

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.

Figure 17 | Year-on-year score changes (2017 to 2018), telecommunications companies



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

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).

Figure 18 | How transparent are telecommunications companies about blocking content and access (F3-F10)?

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

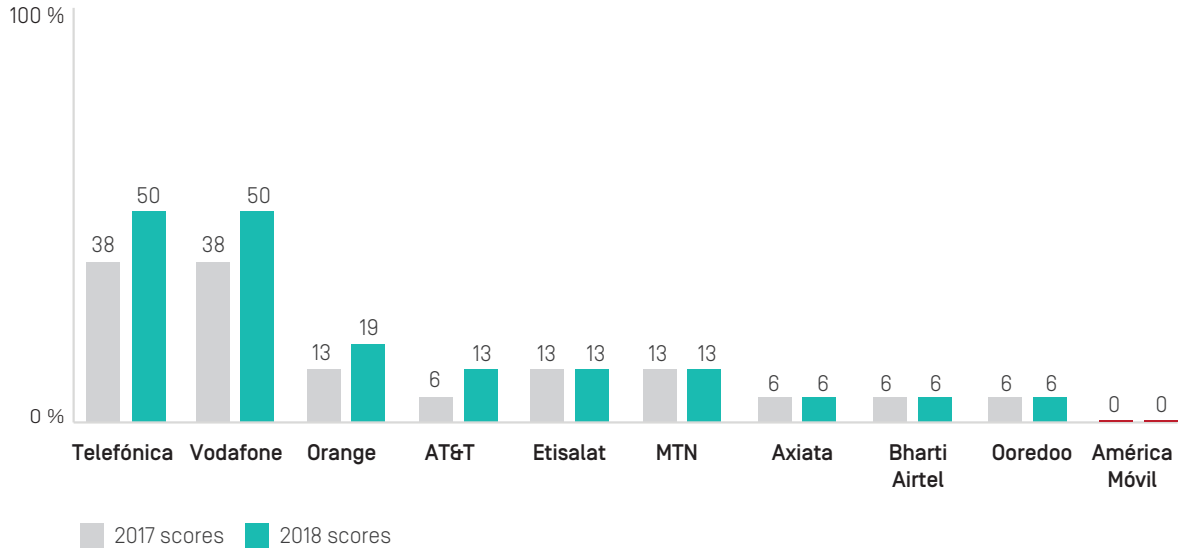
Despite small improvements, a lack of disclosure from companies on network shutdown policies leaves users in the dark about this human rights threat.

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.

Figure 19 | How transparent are telecommunications companies about policies for responding to government shutdown orders (F10)?



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 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.

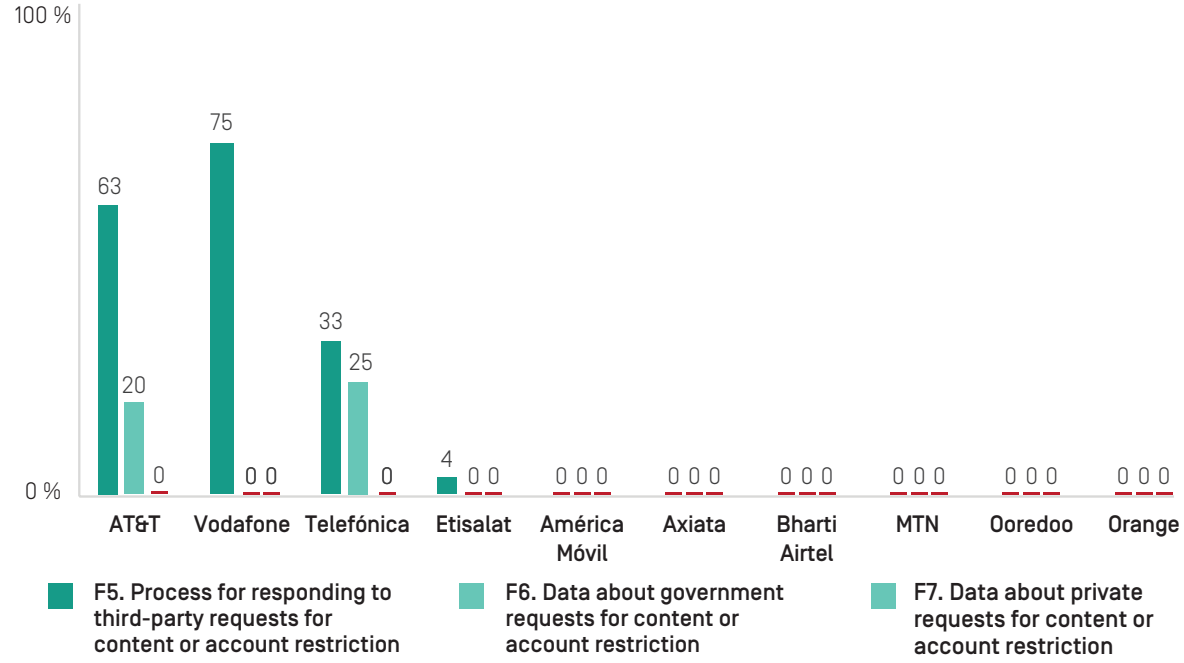
7.3 Policing access to information

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.

Figure 20 | How transparent are telecommunications companies about handling external demands to censor content and restrict accounts (F5-F7)?



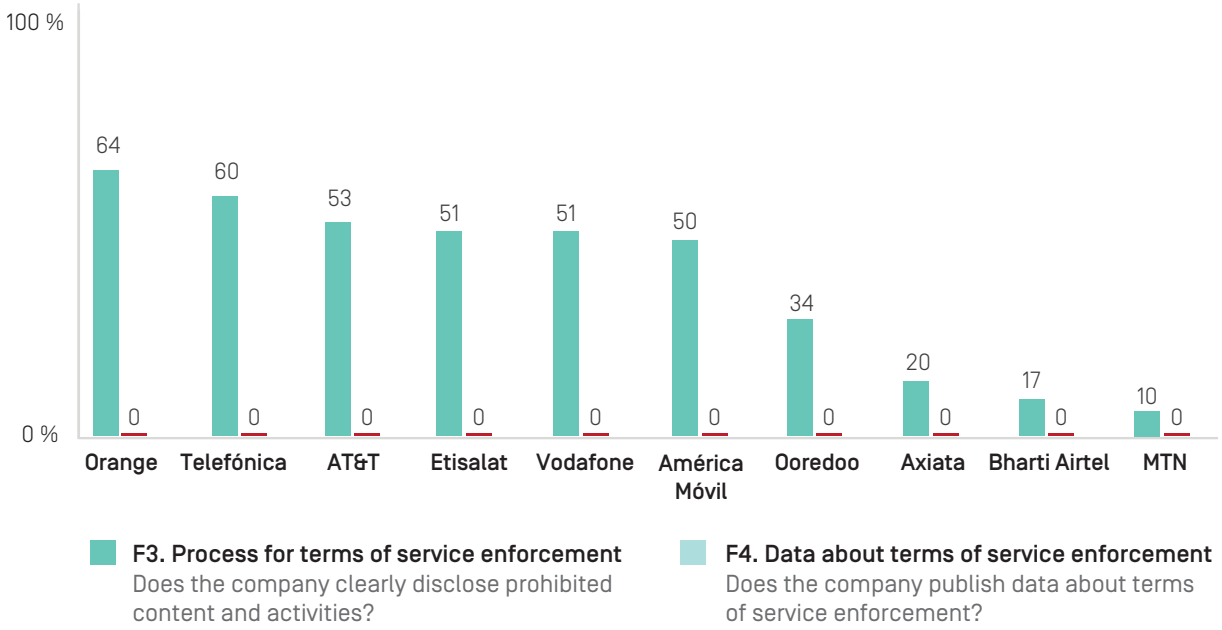
While most telecommunications companies disclosed some information about what types of content or activities are prohibited on their services, none disclosed any information about what actions they take to enforce these terms.

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.

Figure 21 | How transparent are telecommunications companies about their rules and how they are enforced (F3, F4)?



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

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.

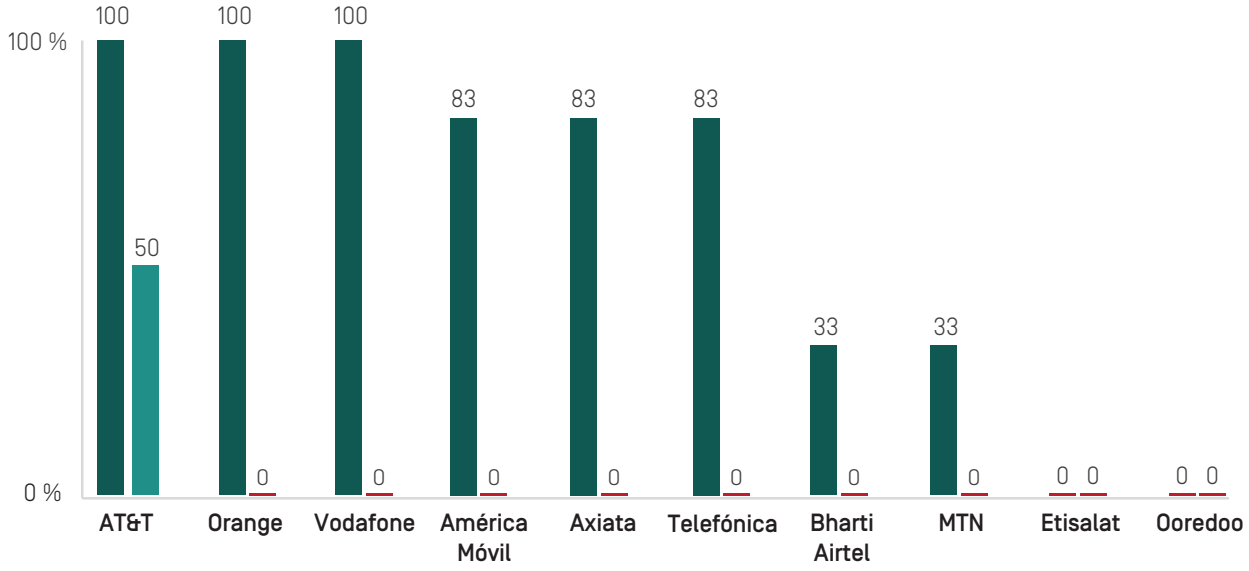
Without transparency about what information is collected, how long it is retained, what is shared with whom, and for what purposes and under whose authority, there is neither accountability nor basic checks against abuse. If people's information is used for surveillance purposes that violate basic international 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.

Figure 22 | Access to and notification about privacy policies (telecommunications companies)



P1. Access to privacy policies
Does the company offer privacy policies that are easy to find, understand, and available in the main languages of its home market?

P2. Changes to privacy policies
Does the company disclose it directly notifies users of changes to privacy policies?

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/.

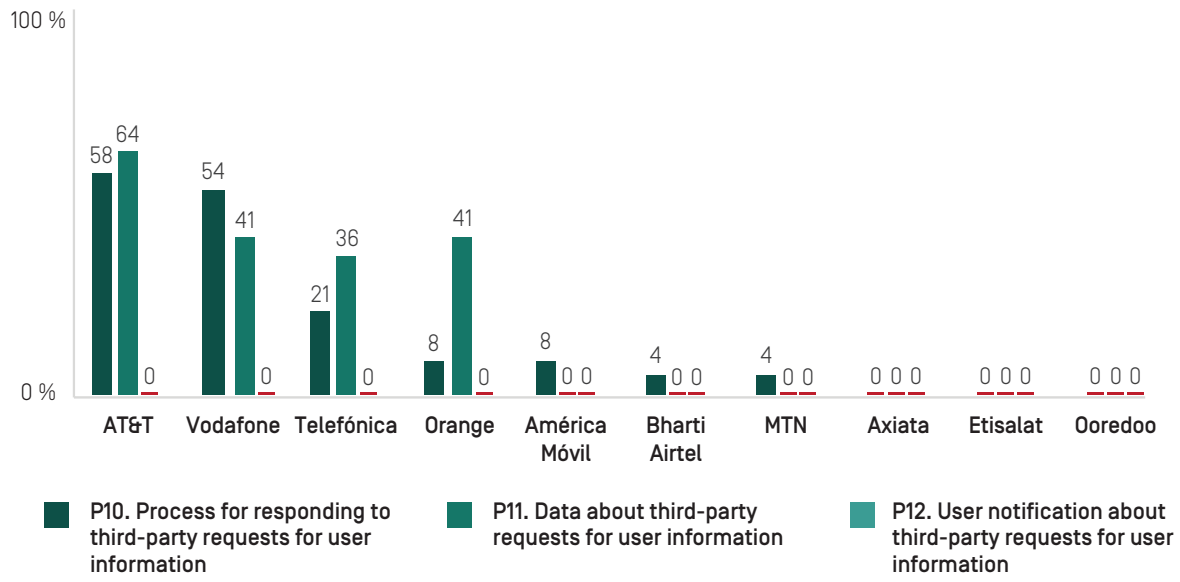
Surveillance accountability: Companies fail to provide maximum, legally permissible transparency about how they handle third-party requests for user information.

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).

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.

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.

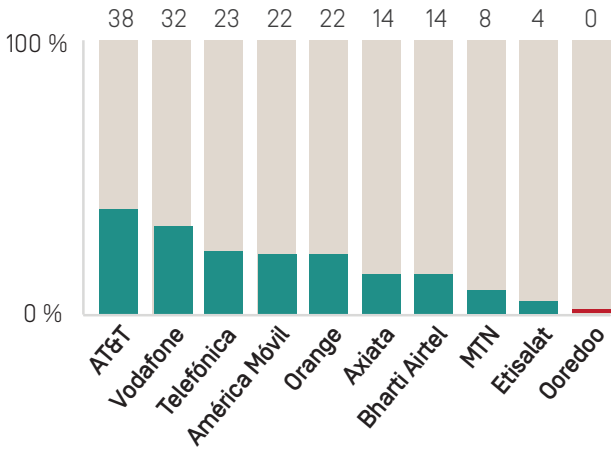
Data protection: Telecommunications companies fail to disclose clear information about collection, use, and sharing of personal information

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).

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

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

- **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.

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.[106]

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?

10. Company report cards

Internet and Mobile Ecosystem Companies

Apple Inc.

SERVICES EVALUATED

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

RANK	SCORE	DIFFERENCE FROM 2017
7	44%	^ 8.02

RANK AMONG 12 INTERNET AND MOBILE ECOYSYSTEM COMPANIES

Key Findings:

- Apple earned the largest score improvement of any company in the Index, but still lagged behind most of its U.S. peers due to its failure to disclose policies affecting users' freedom of expression.
- Apple improved its disclosure of policies affecting users' privacy in a number of areas, including its disclosure of options users have to control how their information is used for targeted advertising. It was also the only company in the Index to clearly disclose that it does not track users across third-party websites.
- Apple improved its disclosure of its policies for responding to data breaches, but its disclosure of other security policies and practices still fell short.

Key Recommendations:

- **Strengthen commitments to freedom of expression.** While the company made significant improvements to its disclosure of policies affecting users' privacy, it needs to improve its disclosure of commitments and policies affecting freedom of expression.
- **Clarify role in policing content.** Apple should disclose more information about its own decisions to remove content that violates the company's terms, as well as data on government requests it receives to remove apps from its app store.
- **Be more transparent about handling of user information.** Apple should clarify what types of user information it collects, shares, and retains, and for what purpose.

Analysis

Apple placed seventh out of the 12 internet and mobile ecosystem companies evaluated, disclosing less about policies and practices affecting freedom of expression than most of its U.S. peers.[1] The company earned the largest score improvement in the 2018 Index, due to improved transparency reporting and disclosure of its policies affecting user privacy. However, Apple still received the lowest score of all U.S. internet and mobile ecosystem companies evaluated due to its lack of disclosure of policies affecting users' freedom of expression. Despite improvements to its transparency reporting, Apple still provided no data about government requests to remove apps from its App Store, or data on content or account restrictions the company undertook to enforce its own rules. U.S. law prevents companies from disclosing the exact number of government requests for stored and real-time user information they receive, which prevented Apple from being fully transparent in that area.[2]

About Apple Inc.

Apple Inc. provides computers, smartphones, and other devices, and also produces iOS operating system software and application software. Services include iMessage, a messaging application that works across Apple devices, and iCloud, a cloud storage service.

Market Cap: USD 906.1 billion[3]
NasdaqGS: AAPL
Domicile: United States
Website: www.apple.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Apple's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/apple.
[2] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.
[3] Bloomberg Markets, Accessed March 14, 2018, https://www.bloomberg.com/quote/AAPL:US.
[4] "Privacy Governance," Apple, accessed March 14, 2018, https://www.apple.com/legal/privacy/en-ww/governance/.

Governance 33%

Apple scored below most of its peers in the Governance category, with the lowest score on this set of indicators of any U.S. company in the Index. Still, the company significantly improved its governance score in the 2018 Index, primarily due to a new "Privacy Governance" policy that more clearly outlines Apple's privacy commitments, though it made no similar clarifications regarding its commitments to freedom of expression.[4] The company strengthened its commitment to respect user privacy as a human right (G1) and clarified its oversight of privacy risks at the senior management level (G2), though it did not publish similar disclosure with regard to freedom of expression. It also disclosed it conducts impact assessments to examine privacy risks associated with its products and services (G4), and that it engages with stakeholders on privacy-related issues (G5). Like its peers, Apple offered little evidence of a substantive grievance and remedy mechanism enabling users to submit complaints against the company for infringement of their freedom of expression or privacy (G6).

Freedom of Expression 30%

Apple revealed little about policies and practices affecting freedom of expression, scoring below all other U.S. companies but performing better than Mail.Ru, Samsung, Yandex, Tencent, and Baidu.

Content and account restrictions: Apple disclosed less than all other internet and mobile ecosystem companies, except for Chinese company Baidu, about what the rules are on its different services and how they are enforced (F3, F4, F8). While it provided some information about what is prohibited (F3), it disclosed no data about the volume or nature of content or accounts it restricted to enforce its rules (F4). It also did not disclose whether it has a policy to notify users when it restricts content or accounts (F8).

Content and account restriction requests: Apple significantly improved its disclosure of how it handles government and private requests to restrict content or accounts (F5-F7), but still disclosed less than its U.S. peers. It disclosed its processes for responding to government requests (F5), and provided data on the number of account restriction requests it received from governments, broken down by country (F6). But it failed to provide data on requests it received to remove content, such as apps from its App Store. It also disclosed nothing about requests it received through private processes (F7).

Identity policy: Users and app developers access Apple services using an Apple ID account. Apple disclosed it might require Apple ID users in certain jurisdictions to verify their identity with their government-issued identification, in compliance with local law (F11).

Privacy 54%

Apple received the third-best score among internet and mobile ecosystem companies in the Privacy category, disclosing less than Google and Microsoft, but more than Twitter and Facebook.

Handling of user information: Like its peers, Apple fell short of clearly explaining how it handles user information (P3-P9). The company did not fully disclose each type of user information it collects (P3), shares (P4), for what purpose (P5), and for how long it retains it (P6). The company improved its disclosure of options users have to control how their information is used for advertising purposes (P7), but this suggests that targeted advertising is on by default. Apple was the only company in the Index to clearly disclose that it does not track users across third-party websites (P9).

Requests for user information: Apple disclosed less than Google and Microsoft but more than the rest of its peers about its process for handling government and private requests for user information (P10-P12). Like most companies, Apple disclosed information about its process for responding to government requests but nothing about private requests it receives (P10). It disclosed data on the number of government requests it received by country, requests it received via court orders, and requests for content vs. non-content data (P11). However, Apple did not disclose the exact number of requests received for stored or real-time user data, or what actions it took in response to these requests, because it is prohibited by law from doing so.[5]

Security: Apple disclosed more than any other internet and mobile ecosystem company other than Google about its security policies, but still fell short in key areas. It did not adequately disclose its internal security oversight processes, including whether it commissions external security audits on its products and services (P13). However, it made notable improvements to its disclosure of how it handles data breaches, and was the only internet and mobile ecosystem company to receive any credit on this indicator (P15).

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

● Internet and Mobile Ecosystem Companies

Baidu, Inc.

RANK	SCORE	DIFFERENCE FROM 2017
12	17%	^ 2.68

RANK AMONG 12 INTERNET AND MOBILE ECOYSYSTEM COMPANIES

SERVICES EVALUATED

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

Key Findings:

- Baidu earned the lowest score of all internet and mobile ecosystem companies in the Index, disclosing almost nothing about policies affecting freedom of expression and privacy.
- Baidu disclosed less about its process for censoring content and restricting user accounts than any other internet and mobile ecosystem company evaluated.
- Baidu improved its disclosure of how it handles user information, including disclosure of the types of user information it may collect, but disclosed less about privacy-related policies than any of its peers.

Key Recommendations:

- **Be more transparent about security policies.** Baidu should improve its disclosure of what it does to keep user information secure, including by communicating its policies for responding to data breaches.
- **Increase transparency about private requests.** Baidu can improve its disclosure about its processes for responding to private requests to restrict content or accounts and for user information.
- **Improve grievance and remedy mechanisms.** Baidu should disclose clear mechanisms for users to submit complaints related to freedom of expression and privacy.

Analysis

Baidu earned the lowest score of all internet and mobile ecosystem companies evaluated, disclosing almost no information about its policies and practices affecting users' freedom of expression and privacy.[1] The company improved its disclosure of its handling of user information, including its disclosure of options users have to control if their information is used for targeted advertising. However, the company still fell short of meeting basic benchmarks for protecting users' freedom of expression and privacy. While the Chinese internet environment is one of the most restrictive in the world,[2] Baidu can still improve its transparency about basic policies affecting freedom of expression and privacy in key areas. The fact that Tencent outperformed Baidu on several such indicators shows that Baidu's poor performance cannot be attributed to China's restrictive legal and political environment alone.

About Baidu Inc.

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

Market Cap: USD 87.3 billion[3]
NasdaqGS: BIDU
Domicile: China
Website: www.baidu.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. See Baidu's performance in the 2017 Index: https://rankingdigitalrights.org/index2017/companies/baidu.
[2] "Freedom on the Net" (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/china.
[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/BIDU:US.

Governance 5%

Baidu scored lowest of all internet and mobile ecosystem companies in the Governance category. The company made a commitment to respect users' privacy, although it fell short of committing to protect privacy as a human right (G1). The company disclosed no evidence of senior-level oversight on freedom of expression or privacy issues (G2), or of employee training or a whistleblower program related to these issues (G3). It failed to disclose if it conducts human rights due diligence (G4), or if the company engages with stakeholders on freedom of expression or privacy issues (G5). China's political and legal environment strongly discourages companies from making human rights commitments, but Baidu could still improve its disclosure of grievance and remedy mechanisms (G6).

Freedom of Expression 12%

Baidu disclosed less about its policies affecting users' freedom of expression than any other internet and mobile ecosystem company evaluated, including Tencent.

Content and account restrictions: Baidu disclosed less than all other internet and mobile ecosystem companies about the rules pertaining to different services and how they are enforced (F3, F4, F8). The company received some credit for its disclosure of what types of content or activities it prohibits on its services (F3), but disclosed no data about the volume and nature of content or accounts it restricts for violating these rules. Baidu did not commit to notify users when their content or accounts have been censored (F8).

Content and account restriction requests: Baidu was one of only two internet and mobile ecosystem companies to receive no credit on these indicators, along with Samsung (F5-F7). It did not disclose any information about its process for responding to government or private requests to restrict content or accounts (F5), nor did it publish data about the requests it received and with which it complied (F6, F7).

Identity policy: The company disclosed it requires users to verify their identities for all services (F11). Service providers offering internet access or information-related services in China are legally required to do so, as are messaging apps.[4]

Privacy 23%

Baidu received the lowest privacy score among all internet and mobile ecosystem companies, including Tencent, despite making some key improvements.

Handling of user information: Baidu disclosed less than almost all other internet and mobile ecosystem companies, other than the Russian internet company Mail.Ru, about how it handles user information (P3-P9). It provided relatively strong disclosure of the types of user information it may collect, on par with Oath, Tencent, and Twitter (P3), but gave significantly less information about what it shares (P4). Baidu improved its disclosure about whether it combines user information from various services and why it does so (P5) and about the user information it retains (P6). While the company improved its disclosure of options users have to control if their information is used for targeted advertising (P7), this suggests that targeted advertising is on by default.

Requests for user information: Baidu disclosed almost nothing about how it handles government and private requests for user information, scoring just above Tencent (P10-P12). Although the Chinese legal and political environment makes it unrealistic to expect companies to disclose most information about government requests, Baidu should be able to reveal if and when it shares user information via private requests and under what circumstances. The company did not disclose whether it notifies users when it receives government or private requests for their information (P12).

Security: Baidu disclosed the least of all internet and mobile ecosystem companies about its security policies (P13-P18). Baidu disclosed nothing about its internal security oversight processes (P13) or the company's policies for responding to data breaches (P15). The company disclosed a bug bounty program through which security researchers can report vulnerabilities, although it did not disclose a time frame in which it will review these reports (P14). Baidu disclosed no information about encryption of user communications (P16). Chinese companies are required by law to provide user information when requested by government authorities, effectively prohibiting them from offering end-to-end encryption or requiring that they provide decryption assistance.[5]

[4] Access Now Policy Team, "A Closer Look at China's Cybersecurity Law - Cybersecurity, or Something Else?," Access Now, December 13, 2017, https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/.
[5] "Antiterrorism Law of 2015," *Xinhuanet.com*, December 27, 2015, http://news.xinhuanet.com/politics/2015-12/27/c_128571798.htm.

● Internet and Mobile Ecosystem Companies

Facebook, Inc

SERVICES EVALUATED

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

RANK

4

SCORE

55%

DIFFERENCE FROM 2017

^ 2.11

RANK AMONG 12 INTERNET AND MOBILE ECOYSYSTEM COMPANIES

Key Findings:

- Facebook ranked fourth in the Index, disclosing less about policies affecting freedom of expression and privacy than several of its U.S. peers.
- The company provided users with limited options to control what information the company collects, retains, and uses, including for targeted advertising, which appears to be on by default.
- Facebook disclosed slightly more information about its processes for identifying and removing content that violates its rules. It provided some data on content restricted for violating rules on hate speech and inauthentic accounts, but still lacked transparency on how it enforces its rules.

Key Recommendations:

- **Commit to user privacy.** The company should show a stronger commitment to protect privacy by not sharing users' information for targeted advertising unless they opt in. Otherwise, the company should clearly disclose that targeted advertising is on by default, and improve mechanisms for user control over their information.
- **Clarify role in policing online content.** Facebook should be more transparent about how it enforces its terms of service by disclosing how it identifies content or activities that violates the rules, and publish data about the type and volume of content it removes for breaching its terms of service.
- **Be more transparent about external requests.** The company should be more transparent about how it responds to government and private requests to hand over user information or remove content.

Analysis

Facebook ranked fourth out of 12 internet and mobile ecosystem companies evaluated, below Google, Microsoft, and Oath, but above Twitter and Apple.[1] As a member of the Global Network Initiative (GNI), Facebook publicly committed to respect human rights, but disclosed less about its policies and practices affecting freedom of expression and privacy than many of its peers. It improved its disclosure of its terms of service enforcement, security measures for WhatsApp and Instagram, and how it handles government requests for user information. U.S. law prohibits companies from disclosing the exact number of government requests for stored and real-time user information they receive, which prevented Facebook from being fully transparent in that area.[2] However, Facebook disclosed less than many of its peers about its handling of user information and options users have to control the data it collects and shares, including for purposes of targeted advertising. Facebook disclosed options for users to opt out of targeted advertising, suggesting that targeted advertising is on by default.

About Facebook, Inc.

Facebook, Inc. operates social networking platforms for users globally. These include the Facebook social network, Messenger, Instagram, and WhatsApp.

Market Cap: USD 536.9 billion[3]
NasdaqGS: FB
Domicile: United States
Website: www.facebook.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index.For Facebook's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/facebook.
[2] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.
[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/FB:US.

Governance 80%

Facebook received the second-highest governance score of the 12 internet and mobile ecosystem companies evaluated, behind Microsoft and Oath. Facebook provided evidence that senior leadership exercises oversight over issues related to freedom of expression and privacy (G2) and that there are mechanisms in place formalizing these commitments throughout the company (G3). It disclosed that it conducts regular human rights impact assessments, though it failed to disclose whether it assesses the risks to freedom of expression and privacy associated with how it enforces its terms of service (G4).

Freedom of Expression 49%

Facebook ranked fifth out of 12 internet and mobile ecosystem companies in the Freedom of Expression category, below most other U.S. companies, but above Oath and Apple.

Content and account restrictions: Facebook improved its disclosure of the processes it uses to identify content or accounts violating its rules (F3) and was one of only four companies to disclose any data about the actions it took to enforce its terms of service (F4). However, Facebook's disclosure still fell short of Index benchmarks for these indicators. Additionally, Facebook did not clearly disclose whether it notifies users when content has been restricted or removed and why (F8).

Content and account restriction requests: Facebook scored in the top half of internet and mobile ecosystem companies on these indicators, though it disclosed less than Google, Oath, and Twitter (F5-F7). Facebook improved its disclosure of its process for responding to removal requests via court orders (F5), and its transparency reporting on private requests for content removal (F5, F7). It disclosure of data on its compliance with government and private requests was less comprehensive (F6, F7). It disclosed actions it took to restrict content in response to government requests but did not disclose the number of requests it received, making it difficult to determine its compliance rate for responding to such requests.

Identity policy: WhatsApp and Instagram disclosed that users can register for an account without verifying their identity with a government-issued ID; however, Facebook's social network and Messenger app disclosed they may require users to do so (F11).[4]

Privacy 49%

Facebook received the seventh-highest score out of 12 internet and mobile ecosystem companies in the Privacy category, behind all other U.S. internet and mobile ecosystem companies and South Korean internet company Kakao.

Handling of user information: Facebook fell short of explaining how it handles user information, placing behind Twitter, Google, Microsoft, Oath, Apple, and Kakao on these indicators (P3-P9). While the company offered some disclosure of what types of user information it collects (P3), it revealed less about what it shares and with whom (P4), for what purpose (P5), and for how long it retains user information (P6). Its disclosure of options users have to control what information the company collects, retains, and uses was worse than any other company in the Index (P7). The company offered some ways to opt out of targeted advertising, suggesting it is on by default. Facebook also did not clearly disclose if it tracks users across the internet using cookies or widgets, or whether it respects user-generated signals to opt out of data collection (P9).

Requests for user information: Facebook disclosed less than Microsoft and Google about its process for handling government and private requests for user information (P10). However, it received the highest score of internet and mobile ecosystem companies, along with Twitter, for its disclosure of data about its compliance with these types of requests (P11). Like most U.S. companies, Facebook disclosed that it notifies users of government requests for their information, and disclosed the circumstances in which it may not notify users, but did not offer similar disclosure of private requests (P12).

Security: Facebook disclosed less than many of its peers, including Google, Apple, and Oath, but more than Twitter, about its security policies (P13-P18). It revealed little about its processes for keeping its products and services secure (P13). Facebook received higher than average marks for disclosure of its encryption policies (P16). The company clearly stated that for WhatsApp, end-to-end encryption is enabled by default, and that Messenger users can enable end-to-end encrypted "secret conversations," although these are not on by default. Facebook improved its disclosure of account security practices by rolling out two-factor authentication for Instagram and WhatsApp (P17).

[4] "Help Center - What Types of ID Does Facebook Accept?" Facebook, accessed March 13, 2018, +https://www.facebook.com/help/159096464162185?helpref=faq_content.

● Internet and Mobile Ecosystem Companies

Google Inc.

SERVICES EVALUATED

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

RANK	SCORE	DIFFERENCE FROM 2017
1	63%	^ 0.52

RANK AMONG 12 INTERNET AND MOBILE ECOYSYSTEM COMPANIES

Key Findings:

- Google disclosed more about policies affecting freedom of expression and privacy than other internet and mobile ecosystem companies in the Index, although it still falls short in key areas.
- The company disclosed less than its Global Network Initiative (GNI) peers about implementation and oversight of its commitments to users' rights, and lacked clear grievance and remedy mechanisms.
- Google improved disclosure of options users have to control their own information, and of how it tracks users across the internet. It disclosed options for users to opt out of targeted advertising, suggesting that targeted advertising is on by default.

Key Recommendations:

- **Do more to protect privacy.** Google should do more to protect privacy by clarifying what information it collects, shares, and for what purpose, and committing to not share users' information for advertising unless they opt in.
- **Be transparent about policing of content.** The company should disclose comprehensive data on content and account removals due to violations of the company's terms of service.
- **Provide better avenues for redress.** The company should improve mechanisms for how users can submit complaints when they believe the company has violated their rights.

Analysis

Google earned the highest score among internet and mobile ecosystem companies, disclosing more information about policies and practices affecting users' freedom of expression and privacy than its peers.[1] A member of the Global Network Initiative (GNI), Google made clear commitments to freedom of expression and privacy, despite gaps in implementation and oversight. The company improved disclosure of privacy-related policies by clarifying options users have to control what information the company collects about them, including whether the company tracks users across third-party websites. However, there is much room for improvement. Google could improve grievance and remedy options, in line with its GNI peers. It could disclose more comprehensive data about its terms of service enforcement. While Google disclosed more than any company in the Index about how it handles government requests for user information, U.S. law prohibiting companies from disclosing the exact number of government requests for stored and real-time user information prevented the company from being fully transparent about these types of requests.[2]

About Google, Inc.

Google Inc. (a subsidiary of Alphabet Inc.) is a global technology company with services that include the Google search engine; Gmail, an email service; and YouTube, a video-sharing platform. It also provides consumer hardware products, and systems software, like its open-source mobile operating system, Android.

Market Cap: USD 783.9 billion[3] (Alphabet Inc.)
NasdaqGS: GOOGL
Domicile: United States
Website: www.google.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Google's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/google.
[2] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.

Governance 72%

Google ranked fourth among internet and mobile ecosystem companies in the Governance category, disclosing less than all of its GNI peers. While it articulated a clear commitment to uphold users' freedom of expression and privacy rights (G1), Google did not disclose evidence of board- or executive-level oversight over these issues (G2). The company committed to conduct human rights due diligence when entering new markets, but researchers were not able to locate evidence that it conducts assessments of risks associated with the processes and mechanisms used to enforce its terms of service (G4). There is also significant room for improvement in terms of the company's grievance and remedy mechanisms when users believe their freedom of expression or privacy rights have been violated (G6).

Freedom of Expression 59%

Google placed second in this category, disclosing more about policies affecting freedom of expression than all other internet and mobile ecosystem companies, apart from Twitter.

Content and account restrictions: Google disclosed less than Twitter, Kakao, and Microsoft but more than the rest of its peers about its content moderation policies and practices (F3, F4, F8). It provided detailed information about what types of content and activities it prohibits, including some information about its processes for identifying content and activities that violate the company's terms of service (F3). Google was one of four companies evaluated to disclose any data about content or accounts it restricted for terms of service violations, but this data is not comprehensive (F4).[4]

Content and account restriction requests: Google disclosed more than any other internet and mobile ecosystem company about how it handles government and private requests to restrict content and accounts (F5-F7). Its transparency report included detailed data about government requests to restrict content or accounts (F6). However, Google's disclosure of data about private requests was significantly less detailed than that of Kakao, Twitter, Microsoft, and Oath (F7).

Identity policy: While for Gmail, YouTube, and Google Play, users are not required to confirm their identity, app developers are required to do so (by making a small financial transaction).

Privacy 63%

Google earned the highest privacy score among internet and mobile ecosystem companies, though it did not lead on all indicators.

Handling of user information: Google disclosed more than most of its peers other than Twitter about how it handles user information, but fell short in key areas. The company provided some information about what user information it collects (P3) but was less transparent than most of its peers about what it shares (P4). It improved disclosure of options users have to control information the company collects about them, including for the purposes of targeted advertising, which suggested that targeted advertising is on by default (P7). The company also clarified options users have to control whether and how it tracks users across third-party websites (P9).

Requests for user information: Google disclosed as much as Microsoft about how it handles government and private requests for user information (P10, P11). It demonstrated a clear commitment to challenge overbroad government requests, and provided clear examples and guidance of how it handles these requests. The company disclosed it notifies users when government officials request their information, but it was not clear about whether it does so in the case of private requests for user information (P12).

Security: Google disclosed more than any other internet and mobile ecosystem company about its security measures (P13-P18). It received full credit for disclosing that it has internal mechanisms in place to secure user information from unauthorized access (P13), and earned the highest score for disclosure of its encryption policies (P16). Like most companies, Google disclosed nothing about its notification and remedy policies in the event of a data breach (P15).

[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/GOOGL:US.
[4] "Why Flagging Matters," Official YouTube Blog, September 15, 2016, https://youtube.googleblog.com/2016/09/why-flagging-matters.html.

Kakao Corp.

SERVICES EVALUATED

- Daum Search (Search engine)
- Daum Mail (Email)
- KakaoTalk (Messaging & VoIP)

RANK: 6

SCORE: 49%

DIFFERENCE FROM 2017: ^ 0.25

RANK AMONG 12 INTERNET AND MOBILE ECOYSYSTEM COMPANIES

Key Findings:

- Kakao disclosed more about policies affecting freedom of expression and privacy than many of its peers, but still fell short in key areas.
- The company disclosed more than some U.S. companies, including Apple, about policies affecting freedom of expression.
- Kakao disclosed little about its handling of security vulnerabilities and how it addresses data breaches.

Key Recommendations:

- **Be more transparent about policing of content.** The company should disclose data about the volume and nature of content or accounts it restricts for terms of service violations.
- **Be more transparent about handling of user information.** Kakao should improve its disclosure of whether and how it collects data by tracking users across the internet.
- **Communicate more clearly about security.** The company should disclose more about its security policies and practices, including its policies for responding to data breaches.

Analysis

Kakao ranked sixth out of the 12 internet and mobile ecosystem companies evaluated, and failed to disclose sufficient information about policies and practices affecting freedom of expression and privacy.[1] However, the company performed better than many companies in the Index, including Apple, and continued to outperform Samsung, the other South Korean internet and mobile ecosystem company evaluated, by roughly 21 points. Notably, South Korean law, such as requirements for grievance mechanisms, helped to boost the company's performance. However, regulatory factors prevented disclosure in other areas. For example, laws requiring companies to remove copyrighted and defamatory content make it difficult to disclose information about certain types of lawful requests to remove or restrict content. Kakao would benefit from a clearer explanation to users about how the law affects what it does not disclose.

About Kakao Corp.

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

Market Cap: USD 8.7 billion[2]
KOSDAQ: A035720
Domicile: South Korea
Website: www.kakao.com

1 The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Kakao's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/kakao.
2 Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/035720:KS.

Governance 35%

Kakao ranked sixth out of the 12 internet and mobile ecosystem companies in the Governance category, below five U.S.-based companies, but scored higher than Apple. It disclosed a commitment to engage with stakeholders (G5) and more about its grievance and remedy processes (G6) than any other internet and mobile ecosystem company evaluated. While this is largely due to requirements under South Korean law, Kakao went beyond the legal requirements by providing users with an appeals mechanism for when content is removed in response to defamation claims. However, the company disclosed little regarding its implementation of human rights impact assessments on potential risks to freedom of expression and privacy (G4).

Freedom of Expression 55%

Kakao received the third-highest freedom of expression score among internet and mobile ecosystem companies, behind Twitter and Google.

Content and account restrictions: Kakao led most of its peers in its clarity about what types of content and activities are prohibited across its services (F3, F4, F8). However, while Kakao disclosed more than most of its peers, on par with Microsoft, about what its rules are and its processes for enforcing them (F3), it disclosed no data about the volume or type of content removed or accounts deactivated as a result of terms of service violations (F4). The company earned the second-highest score after Twitter for its clear policies about notifying users when it removes content or restricts accounts (F8).

Content and account restriction requests: Kakao disclosed less than Google, Oath, Twitter, and Facebook about its handling of government and private requests to remove content or restrict accounts, but it provided more information than Microsoft and Apple (F5-F7). Disclosure of its processes for responding to government and private requests (F5) was slightly above average, although disclosure of government requests was weaker than about private requests. Notably, the company did not provide data about government requests to restrict content or accounts from outside of South Korea (F6). Kakao disclosed more data than its peers, except for Twitter, about private requests it receives to block content or restrict user accounts (F7).

Identity policy: Kakao stated it may require users to verify their identities with their phone number or an official ID in order to access some services (F11).

Privacy 51%

Kakao received the sixth-best privacy score of the 12 internet and mobile ecosystem companies evaluated, falling behind five U.S.-headquartered companies, but scoring higher than Facebook.

Handling of user information: Kakao disclosed less than most U.S. companies but more than Facebook about its handling of user information (P3-P9). Notably, Kakao received the highest score of any company in the Index for its disclosure of what types of user information it collects and shares (P3, P4), but was less transparent about its purpose for doing so (P5). While the company improved its disclosure of options KakaoTalk users have to control how their user information is used for targeted advertising, this suggested that targeted advertising is on by fault (P7). Kakao also disclosed nothing about whether it tracks users across the internet (P9).

Requests for user information: Kakao disclosed less about how it handles government and private requests for user information than all U.S. internet and mobile ecosystem companies evaluated, but more than the rest of its peers (P10, P11). It provided no information about whether it notifies users of government or private requests for their information (P12).

Security: Kakao ranked in the top half of internet and mobile ecosystem companies on its disclosure of its security policies, though it offered less disclosure than Google, Apple, Yandex, and Microsoft (P13-P18). It received full credit, along with Google, for disclosing what internal measures it takes to secure users' information (P13). However, it provided little information about measures taken to address security vulnerabilities (P14) or about its handling of data breaches (P15). Kakao also disclosed less than most of its peers about its encryption practices across different services (P16).

Mail.Ru Group Limited

SERVICES EVALUATED

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

RANK	SCORE	DIFFERENCE FROM 2017
11	21%	0.00

RANK AMONG 12 INTERNET AND MOBILE ECOYSYSTEM COMPANIES

Key Findings:

- Mail.Ru disclosed less than most other internet and mobile ecosystem companies about policies affecting users' freedom of expression and privacy.
- The company disclosed almost nothing about how it handles government demands to remove content or hand over user data, although it is not illegal to disclose at least some information about its processes for responding to these types of requests.
- The company lacked transparency about what user data it collects and shares, and for what purposes, including for the use of targeted advertising, as well as what measures it takes to keep this data secure.

Key Recommendations:

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

Analysis

Mail.Ru ranked 11th of the 12 internet and mobile ecosystem companies evaluated, disclosing little about policies affecting freedom of expression and privacy. It made no improvements in the 2018 Index.[1] Notably, the company disclosed significantly less about its privacy policies than Yandex, the other Russian company evaluated. While operating in an increasingly restrictive internet environment that discourages companies from publicly committing to protect human rights,[2] the company could be more transparent about key policies and practices affecting freedom of expression and privacy. It could disclose more about its processes for handling government and private demands to restrict content or to hand over user information, as there are no legal obstacles preventing the company from doing so. Mail.Ru could also improve disclosure about its handling of user information—an area in which Yandex was more transparent—and give users clear options to control what information the company collects and shares, including for the use of targeted advertising.

About Mail.Ru Group Limited

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

Market Cap: USD 8.2 billion[3]
LSE: MAIL
Domicile: Russia
Website: http://corp.mail.ru

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Mail.Ru's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/mailru/.
[2] "Freedom on the Net," (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/russia.
[3] Bloomberg Markets, accessed March 8, 2018, https://www.bloomberg.com/quote/MAIL:LI.

Governance 7%

Mail.Ru scored poorly in the Governance category, tying with Yandex and Tencent for the second-lowest score among internet and mobile ecosystem companies. The company received some credit on just two of the six indicators in this category. It disclosed a whistleblower program, but not specifically for reporting freedom of expression and privacy concerns (G3), and disclosed a grievance mechanism for complaints related to freedom of expression, but not for privacy issues (G6).

Freedom of Expression 22%

Mail.Ru disclosed little about policies affecting users' freedom of expression, tying with Samsung for the fourth-lowest score of internet and mobile ecosystem companies, ahead of Yandex, Tencent, and Baidu.

Content and account restrictions: Mail.Ru disclosed more than Yandex but less than other internet and mobile ecosystem companies about what the rules are and how they are enforced (F3). Like most companies in the Index, Mail.Ru disclosed no data about the volume and nature of content or accounts it restricts for terms of service violations (F4). Unlike Yandex, Mail.Ru did not disclose if it notifies users when it restricts content or their accounts (F8).

Content and account restriction requests: Mail.Ru disclosed almost nothing about its process for handling government and private requests to block content or user accounts (F5-F7). The company provided only minimal information about its processes for responding to these types of requests (F5), and offered no data about the number of government or private requests it received or complied with (F6, F7), although there are no laws prohibiting Mail.Ru from doing so.

Identity policy: Mail.Ru's VKontakte, the social networking service, disclosed a requirement for users to provide a mobile phone number and to verify a user's real identity in case a user needs tech support. Internet service providers, telecommunications companies, and instant messaging services in Russia are legally required to verify the identities of their users, but it is unclear if the regulations apply to social network platforms like VKontakte.[4]

Privacy 25%

Mail.Ru received the second-lowest privacy score of the 12 internet and mobile ecosystem companies, scoring better than only Baidu.

Handling of user information: Mail.Ru disclosed less than all other internet and mobile ecosystem companies, including Yandex, about its handling of user information (P3-P9). While the company disclosed some information about what types of user data it collects (P3), shares (P4), and for what purpose (P5), it revealed little about for how long user information is retained (P6). Mail.Ru also lacked clarity about what options users have to control the company's collection of their data, including options to control how their information is used for targeted advertising (P7), or whether the company tracks users across the internet with cookies or widgets (P9).

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

Security: Mail.Ru disclosed little about its security policies, but more than four other internet and mobile ecosystem companies, including Twitter (P13-P18). Like most companies, it offered no information about its process for responding to data breaches (P15). It also disclosed little about its encryption policies, particularly in comparison to Yandex, the other Russian internet company evaluated (P16).

[4] "Law on Communications," No. 126-FZ (2003), as amended by Federal Law N 304-FZ in 2013, and "Amendments to Articles 10.1 and 15.4 of the Federal Law on Information, Information Technologies and Information Protection," No. 241-FZ (2017).
[5] Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," *The Guardian*, September 8, 2015, http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

● Internet and Mobile Ecosystem Companies

Microsoft Corp.

SERVICES EVALUATED

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

RANK	SCORE	DIFFERENCE FROM 2017
2	61%	▼ 0.42

RANK AMONG 12 INTERNET AND MOBILE ECOSYSTEM COMPANIES

Key Findings:

- Microsoft was one of the top performers in the 2018 Index, placing second after Google.
- Microsoft tied with Oath for the most disclosure of governance processes aimed at ensuring the company's respect for freedom of expression and privacy.
- While its disclosure of how it handles government and private requests for user information was among the highest in the Index, Microsoft was less transparent than most of its peers about its processes for handling government and private requests to remove content or restrict accounts.

Key Recommendations:

- **Clarify role in policing online content.** Microsoft should disclose more information about how it enforces its rules, and should expand the types of content removals it covers in its transparency reporting.
- **Be more transparent about handling of user information.** Microsoft should more clearly disclose what types of user information it collects, shares, retains, and for what purpose, and provide users with clear options to control collection and sharing of their information.
- **Provide clear commitments to notify users of content or account restrictions.** Microsoft should clearly commit to notify users when content or accounts are restricted, including the reason why.

Analysis

Microsoft earned the second-highest score among internet and mobile ecosystem companies, after Google.[1] A member of the Global Network Initiative (GNI), Microsoft disclosed a strong commitment to freedom of expression and privacy. Despite its overall strong performance, its score declined slightly as a result of policies for notifying Skype users if the company restricts their accounts being no longer available. In addition, Microsoft could be more transparent about its process for enforcing its terms of service and could clarify how it handles user information, including options users have to control what information about them is collected and shared. U.S. law prevents companies from disclosing the exact number of government requests for stored and real-time user information they receive, which prevented Microsoft from being fully transparent in that area.[2] However, Microsoft still disclosed more data on government and private requests for user information than most companies in the Index.

About Microsoft Corp.

Microsoft Corp. develops, licenses, and supports software products, services, and devices worldwide. Major offerings include Windows operating system, Microsoft Office, Windows Phone software and devices, advertising services, server products, Skype, and Office 365 cloud services.

Market Cap: USD 724.2 billion[3]
NasdaqGS: MSFT
Domicile: United States
Website: www.microsoft.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index.For Microsoft's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/microsoft.
[2] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.
[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/MSFT:US.

Governance 88%

Microsoft tied with Oath for the highest governance score of the 12 internet and mobile ecosystem companies evaluated. The company disclosed an explicit commitment to respect freedom of expression and privacy as human rights (G1), evidence of oversight of human rights issues by senior leadership (G2), and employee training and whistleblower programs that address freedom of expression and privacy (G3). Microsoft disclosed that its human rights impact assessments included efforts to address freedom of expression and privacy risks associated with how it enforces its terms of service (G4). Like all companies, Microsoft could do more to clarify its grievance and remedy mechanisms enabling users to submit complaints about infringements to their freedom of expression or privacy rights (G6).

Freedom of Expression 52%

Microsoft disclosed less about policies affecting freedom of expression than Twitter, Google, and Kakao.

Content and account restrictions: Microsoft disclosed less than Twitter and Kakao but more than all other internet and mobile ecosystem companies about its rules and how they are enforced (F3, F4, F8). Its score declined slightly due to information for notifying Skype users in the event of an account restriction being no longer available on the Skype help page (F8). Microsoft was one of four companies to publish some data about its terms of service enforcement (F4), specifically on content removed from Bing for violating its policy on "non-consensual pornography." However, the company should disclose data on other types of content it removes for terms of service violations.

Content and account restriction requests: Microsoft disclosed more than most internet and mobile ecosystem companies about how it responds to government and private requests to remove content or restrict accounts, but provided less information than Google, Oath, Kakao, Twitter, and Facebook (F5-F7). It disclosed some information about the company's process for responding to government and private requests to remove content (F5), and some data about the number of these requests it received and with which it complied (F6, F7).

Identity policy: Microsoft and Twitter were the only two internet and mobile ecosystem companies to disclose that they do not require users to verify their identity with a form of government-issued ID (F11).

Privacy 56%

Microsoft disclosed more than the rest of its peers, apart from Google, about policies affecting users' privacy.

Handling of user information: Microsoft disclosed less than Twitter, Google, and Oath about how it handles user information (P3-P9). The company did not fully disclose the types of user information it collects, shares, or for what purpose (P3, P4, P5). Like most companies, it provided even less information about how long it retains this information (P6). It also disclosed some options users have to opt out of whether their information is collected for targeted advertising, which suggests that targeted advertising is on by default (P7). It disclosed more than most companies about options users have to obtain information the company holds about them (P8), and whether and how the company collects information about users across third-party websites (P9), though this disclosure still fell short.

Requests for user information: Microsoft disclosed more than its peers about its process for handling government and private requests for user information (P10), but lagged behind Twitter, Facebook, and Google on disclosure of data on the requests it received (P11). Microsoft disclosed its policy for notifying users about government requests for their user information, but not for requests it receives through private processes (P12).

Security: Microsoft disclosed less than Apple, Google, and Yandex about its security policies, but more than the other internet and mobile ecosystem companies evaluated (P13-P18). It disclosed it conducts internal security audits (P13), and offered a bug bounty program to address security vulnerabilities (P14). Like most companies in the Index, Microsoft failed to disclose policies for responding to data breaches (P15). It scored lower than Facebook, Apple, Yandex, and Google on disclosure of its encryption policies (P16).

Internet and Mobile Ecosystem Companies

Oath, Inc.

SERVICES EVALUATED

- **Yahoo Mail (Email)**
- **Flickr (Video & photo sharing)**
- **Tumblr (Social networking & blog)**

RANK	SCORE	DIFFERENCE FROM 2017
3	59%	^ 1.55

RANK AMONG 12 INTERNET AND MOBILE ECOSYSTEM COMPANIES

Key Findings:

- Oath was one of the top performers of the 2018 Index and showed clear commitments to respect freedom of expression and privacy.
- Oath improved its disclosure of government requests to censor content and hand over user data, and clarified options users have to opt out of targeted advertising.
- The company lacked disclosure of what steps it takes to keep user data secure, including how it handles data breaches.

Key Recommendations:

- **Communicate more clearly about security**. The company should disclose more about its processes for responding to data breaches and preventing unauthorized access.
- **Be more transparent about policing of content.** Oath should disclose data about the volume and nature of content or accounts it restricts for terms of service violations.
- **Be more transparent about external requests affecting user rights.** Oath should improve its disclosure of government and private requests to restrict content or accounts and hand over user information.

Analysis

Oath ranked third out of the 12 internet and mobile ecosystem companies evaluated, behind Google and Microsoft.[1] A member of the Global Network Initiative (GNI), Oath has continued to implement many of the human rights commitments and policies previously established by Yahoo, following Verizon's acquisition of Yahoo and the establishment of Oath in June 2017.[2] The company made several improvements in the 2018 Index, including incorporating Tumblr into Oath's more detailed transparency reporting. While Oath disclosed a strong commitment to respect human rights at the governance level, it could still improve its disclosure of key policies affecting users' freedom of expression and privacy. It could be more transparent about how it polices content on its services and could be more clear about its security practices. Oath disclosed less data than all other U.S. internet and mobile ecosystem companies about the government and private requests it received for user information. U.S. law prohibits companies from disclosing exact numbers of government requests for stored and real-time user information they receive, which prevented Oath from being fully transparent in that area.[3]

About Oath Inc.

Oath Inc. (a subsidiary of Verizon Communications) provides a range of communication, sharing, and information and content services. Following the acquisition of Yahoo by Verizon Communications in June 2017, Verizon combined Yahoo-branded services and AOL-branded services into a new subsidiary called Oath.

Market Cap: USD 200.7 billion[4] (Verizon Communications, Inc.)
NasdaqGS: VZ (Oath is a subsidiary of Verizon)
Domicile: United States
Website: www.oath.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Yahoo's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/yahoo.
[2] "Verizon Closes Yahoo Deal, Mayer Steps down," *Reuters*, June 14, 2017, https://www.reuters.com/article/us-yahoo-m-a-verizon/verizon-closes-yahoo-deal-mayer-steps-down-idUSKBN194220.
[3] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.
[4] Bloomberg Markets, accessed March 14, 2018, https://www.bloomberg.com/quote/VZ:US.

Governance 88%

Oath tied with Microsoft for the highest governance score among internet and mobile ecosystem companies. The company disclosed a clear commitment to freedom of expression and privacy as human rights (G1), evidence of senior leadership oversight of human rights concerns (G2), and employee training and a whistleblower program addressing freedom of expression and privacy (G3). Oath disclosed evidence that it engages with stakeholders, including civil society, on freedom of expression and privacy issues (G5). Disclosure of its human rights due diligence processes (G4) declined slightly since the 2017 Index, due to less clear disclosure of whether its human rights impact assessments (HRIAs) are incorporated into executive- or board-level decisions (G4). Like most companies evaluated, Oath did not disclose sufficient grievance and remedy mechanisms (G6).

Freedom of Expression 48%

Oath received the sixth-highest score of the 12 internet and mobile ecosystem companies evaluated in the Freedom of Expression category, behind Facebook, Google, Kakao, Microsoft, and Twitter.

Restricting content and accounts: Oath was less transparent about its process for enforcing its terms of service (F3) than many of its peers, including Facebook, Google, Kakao, Microsoft, and Twitter. Like most companies, Oath did not disclose any data about the volume or nature of actions it took to enforce its rules, such as removing content or restricting users' accounts (F4). The company clarified and improved policies regarding whether it notifies users of account restrictions (F8).

Content and account restriction requests: Oath disclosed more than all of its peers other than Google about how it handles government and private requests to censor content or restrict accounts (F5-F7). It improved its disclosure due to the inclusion of Tumblr in the parent company's transparency reports, which contained more comprehensive information than Tumblr's previous reports. Like most companies evaluated, Oath provided less thorough disclosure of its processes for content or account restriction requests filed through private processes than it did for government requests (F5).

Identity policy: Tumblr disclosed it does not require users to verify their identities, but for Yahoo Mail and Flickr, the company disclosed that users are required to verify their account with a phone number, which in some jurisdictions can be used by law enforcement or other government officials to connect users with their offline identities (F11).

Privacy 54%

Oath received the third-highest score of the 12 internet and mobile ecosystem companies evaluated in the Privacy category, behind Google and Microsoft and on par with Apple.

Handling of user information: Oath disclosed less than Twitter and Google but more than the other internet and mobile ecosystem companies evaluated about how it handles user information (P3-P9). Oath disclosed more about what user information it collects and shares (P3, P4) than it did about its purpose for doing so (P5). While it improved its disclosure of options users have to opt out of targeted advertising (P7), this suggested that targeted advertising is on by default. Oath offered more information than most of its peers, aside from Google, about whether users can access the information that the company holds about them (P8).

Requests for user information: Oath was less transparent than Google and Microsoft about its process for responding to government and private requests for user information (P10), but disclosed more than the rest of its peers. Oath now includes Tumblr in its transparency reporting, which contained more detailed disclosure of Tumblr's handling of government and private requests for user information. However, Oath disclosed less data than all other U.S. internet and mobile ecosystem companies about the government and private requests it received for user data (P11). Oath did not disclose the exact number of requests received for stored or real-time user data, or what actions it took in response to these requests, because U.S. companies are prohibited by law from doing so.[5] The company disclosed clear policies for notifying users of government requests for their user information, when legally possible, similar to most U.S. companies (P12).

Security: Oath disclosed less about its security policies than Google, Yandex, Microsoft, Kakao, and Apple (P13-P18). It disclosed nothing about its policies for handling data breaches (P15), like most companies in the Index. Oath's disclosure of its encryption practices improved slightly due to a change in Tumblr's disclosure in which the company stated that the transmission of data for Tumblr blogs is encrypted by default (P16).

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

Samsung Electronics Co. Ltd.

SERVICES EVALUATED

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

RANK

8

SCORE

28%

DIFFERENCE FROM 2017

^ 1.93

RANK AMONG 12 INTERNET AND MOBILE ECOSYSTEM COMPANIES

Key Findings:

- Samsung disclosed less than most internet and mobile ecosystem companies about policies affecting users' freedom of expression and privacy.
- The company lacked transparency on how it polices content in its app store and about how it handles demands for user data.
- The company improved its disclosure of options users have to control how their information is used for targeted advertising, but still lacked transparency about its handling of user information in key areas.

Key Recommendations:

- **Provide avenues for redress.** The company should provide comprehensive information about how users can file complaints if their freedom of expression or privacy rights are violated by company practices.
- **Be transparent about external requests.** The company should provide data on how many third party requests it received to restrict content and accounts, as well as requests received to hand over user information.
- **Clarify what user data it collects and shares.** Samsung should be more clear with users about what types of data it collects, shares, and for what purpose, and whether it combines user information across different services.

Analysis

Samsung ranked eighth out of the 12 internet and mobile ecosystem companies evaluated, disclosing less than most of its peers about policies affecting users' freedom of expression and privacy.[1] Despite some improvements in the 2018 Index, the company continued to lag behind Kakao, the other South Korean company evaluated. Samsung improved its disclosure of senior leadership oversight over how policies and practices may affect freedom of expression and privacy, and disclosed new information about its human rights impact assessments. It also improved its disclosure of options users have to control how their information is used for targeted advertising. While South Korea has one of the strongest data protection regimes in the world—for instance, it requires companies to obtain consent from users when collecting and sharing user information—Samsung still lacked clarity about these policies and practices in its public disclosure. Companies are also legally required to offer grievance mechanisms, but Samsung did not publicly disclose clear options for users to submit freedom of expression and privacy-related complaints.

About Samsung Electronics Co. Ltd.

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

Market Cap: USD 283.3 billion[2]
KOSE: A005930
Domicile: South Korea
Website: www.samsung.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Samsung's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/samsung.

Governance 32%

Samsung ranked eighth among internet and mobile ecosystem companies in the Governance category, below Kakao and all U.S.-based internet and mobile ecosystem companies. The company clarified that members of its executive- and management-level teams oversee how its policies and practices may impact privacy (G2), and provided more insight into human rights impact assessments related to privacy risks (G4). However, the company did not disclose a commitment to engage with stakeholders on freedom of expression and privacy issues (G5), and lacked clear disclosure of how users can submit freedom of expression and privacy related grievances (G6).

Freedom of Expression 22%

Samsung disclosed little about its policies affecting users' freedom of expression, ranking eighth out of 12 internet and mobile ecosystem companies in this category, on par with Russian internet company Mail.Ru.

Content or account restrictions: Samsung lacked transparency about its processes for policing content and activities that violate its own rules in its app store, but disclosed more than Apple and several other companies. For both Galaxy users and app developers, Samsung disclosed some information about why it may restrict content or accounts (F3), but disclosed no data about the volume or nature of content or accounts it restricted for violating these rules (F4). Samsung also failed to disclose whether it notifies users who attempt to access content that has been restricted (F8).

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

Identity policy: Samsung disclosed that users and developers are required to submit a government-issued ID or phone number (F11).

Privacy 29%

Samsung disclosed less about its policies affecting users' privacy than most other internet and mobile ecosystem companies evaluated, other than Mail.Ru and Baidu.

Handling of user information: Samsung disclosed less than most other internet and mobile ecosystem companies about its policies for handling user information, scoring higher on these indicators than only Yandex, Baidu, and Mail.Ru (P3-P9). The company was less clear in the 2018 Index about whether it combines user information across different services (P5). Samsung improved its disclosure of options users have to opt-out of targeted advertising, but this suggests that targeted advertising is on by default (P7). It also failed to disclose if it tracks users across third-party websites using cookies, widgets, or other types of tracking tools (P9).

Requests for user information: Samsung was one of three internet and mobile ecosystem companies, including Mail. Ru and Tencent, that disclosed no information about its process for responding to government or private requests for user information (P10). It did not publish any data about such requests it received or with which it complied (P11), and failed to disclose whether it notifies users when their information is requested (P12).

Security: Samsung disclosed little about its security policies compared to its peers (P13-P18). It disclosed a bug bounty program but, like most companies, fell short of committing to refrain from prosecuting security researchers (P14). It disclosed that it receives security updates from Google for its Android operating system, but did not specify a timeframe for delivering updates to users (P14).[3] It disclosed nothing about its policy for responding to data breaches (P15), or about what types of encryption are in place to protect user information in transit or on Samsung devices (P16).

[2] Bloomberg Markets, accessed February 26, 2018, https://www.bloomberg.com/quote/005930:KS.
[3] "Samsung on Android (TM)" (Samsung, 2016), https://kp-cdn.samsungknox.com/b4d72b36cd0bc416d54f9d188ab381a1.pdf.

Tencent Holdings Limited

SERVICES EVALUATED

- QZone (Social networking & blog)
- QQ (Instant messaging & VoIP)
- WeChat (Messaging & VoIP)

RANK

10

SCORE

23%

DIFFERENCE FROM 2017

^ 0.91

RANK AMONG 12 INTERNET AND MOBILE ECOSYSTEM COMPANIES

Key Findings:

- Tencent disclosed little about policies affecting users' freedom of expression and privacy, but was more transparent than Baidu, the other Chinese internet company evaluated.
- Tencent received one of the lowest privacy scores in the Index, although it improved its disclosure of how it handles user information for WeChat.
- The company tied with Facebook and Yandex for the highest score for its disclosure of how it addresses security vulnerabilities, but lacked transparency about other security measures it takes to keep user information secure.

Key Recommendations:

- **Increase transparency about private requests.** Tencent should improve its disclosure of its processes for responding to private requests to restrict content or accounts and for user information.
- **Disclose more information about data retention.** For each type of user information it collects, Tencent should disclose how long it retains that information.
- **Improve grievance and remedy mechanisms.** Tencent should disclose clear mechanisms for users to submit complaints related to freedom of expression and privacy across all services.

Analysis

Tencent ranked 10th out of the 12 internet and mobile ecosystem companies evaluated, disclosing little about its policies and practices affecting freedom of expression and privacy.[1] The Chinese internet environment is one of the most restrictive in the world,[2] which accounts for Tencent's poor performance in some areas. Its score nonetheless increased slightly in the 2018 Index for improved disclosure of its terms of service enforcement for WeChat and for clarifying how that service handles user information. However, there are still areas in which Tencent could improve its disclosure without regulatory change, particularly regarding how it handles and secures user information. Tencent offered different versions of its terms of service and privacy policies for mainland Chinese users than for users outside of China. Versions in English and traditional Chinese characters (applied to non-Chinese users outside of the People's Republic of China) contained different substantive content and commitments in some areas, generally with more detail and better disclosure.[3] In addition, China's surveillance-friendly legal environment does not fully excuse Tencent's lack of basic information about its security practices.

About Tencent Holdings Limited

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

Market Cap: USD 547.2 billion[4]
SEHK: 700
Domicile: China
Website: www.tencent.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Tencent's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/tencent.
[2] "Freedom on the Net" (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/china.
[3] Only the documents in simplified Chinese (for mainland Chinese users) counted towards the company's Index score.
[4] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/700:HK.

Governance 7%

Tencent ranked ninth out of 12 internet and mobile ecosystem companies in the Governance category, ahead of Baidu. The company stated that it values users' privacy,[5] although this was not within the context of privacy as a human right, and the company did not disclose a commitment to respect users' freedom of expression (G1). To the contrary, its terms of service for mainland Chinese users stated that users' accounts may be terminated for using Tencent's services for political activity.[6] The company provided some information about a general complaints mechanism for users that applied to all services, with WeChat providing somewhat more detail than QZone and QQ. While Tencent scored below average on this indicator (G6), it nonetheless scored above Facebook.

Freedom of Expression 14%

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

Content and account restrictions: Tencent disclosed less than most other internet and mobile ecosystem companies about policies for moderating content and accounts on its platforms (F3, F4, F8), but more than Apple and Baidu. The company disclosed some information about the types of content or activities it prohibits, and slightly improved its disclosure for WeChat by including more detailed examples to help users understand its rules (F3). Tencent failed to disclose the volume and nature of content or accounts it restricted when enforcing its rules (F4). It also did not commit to notify affected users when the company censors content or accounts (F8).

Content and account restriction requests: Tencent disclosed almost no information about how it handles government and private requests to censor content or user accounts, although it still scored slightly better on these indicators than Baidu and Samsung (F5-F7). It did not publish any data about government or private requests for content or account restrictions it received or with which it complied (F6, F7).

Identity policy: The company disclosed that it may, depending on applicable laws, require users to verify their identity with a government-issued ID for all services (F11). Network service providers offering internet access or information-related services in China are legally required to do so, as are messaging apps.[7]

Privacy 32%

Tencent received the fourth-lowest privacy score of the 12 internet and mobile ecosystem companies evaluated, ahead of Samsung, Mail.Ru, and Baidu.

Handling of user information: Tencent disclosed less than most of its peers about its policies for handling user information (P3-P9). Tencent disclosed limited information on options users have to control what the company collects about them, including for the purposes of targeted advertising (P7). The company disclosed nothing about how long it retains user information (P6). China's Cybersecurity Law requires companies to retain network logs for at least six months but does not forbid disclosure of that fact.[8]

Requests for user information: Tencent disclosed no information about how it handles government and private requests for user information, scoring slightly lower than Baidu on these indicators (P10-P12). While the Chinese legal and political environment makes it unrealistic to expect companies to disclose most information about government requests for user information, Tencent should be able to divulge if and when it shares user information via private requests and under what circumstances.

Security: Tencent disclosed little about its security policies, scoring better than only Baidu and Samsung on these indicators (P13-P18). However, the company tied with Facebook and Yandex for the highest score for its disclosure on how it addresses security vulnerabilities (P14). Like most other internet and mobile ecosystem companies, Tencent did not disclose any information about how it handles data breaches (P15). It disclosed almost no information about encryption of user communications (P16). Chinese companies are required by law to provide user information when requested by government authorities, effectively discouraging them from offering end-to-end encryption or requiring that they provide decryption assistance.[9]

[5] "Privacy Policy," QQ.com, accessed March 14, 2018, http://www.qq.com/privacy.htm.
[6] "Tencent User Service Agreement," Tencent, accessed March 14, 2018, http://www.qq.com/contract.shtm.
[7] Access Now Policy Team, "A Closer Look at China's Cybersecurity Law - Cybersecurity, or Something Else?," Access Now, December 13, 2017, https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/.
[8] Ibid.
[9] Antiterrorism Law of 2015," *Xinhuanet.com*, December 27, 2015 http://news.xinhuanet.com/politics/2015-12/27/c_128571798.htm.

● Internet and Mobile Ecosystem Companies

Twitter, Inc.

SERVICES EVALUATED

- **Twitter (Social networking & blog)**
- **Periscope (Video & photo sharing)**

RANK	SCORE	DIFFERENCE FROM 2017
5	54%	∧ 4.60

RANK AMONG 12 INTERNET AND MOBILE ECOSYSTEM COMPANIES

Key Findings:

- Twitter disclosed less than most of its U.S. peers about policies affecting users' privacy, but disclosed more about policies affecting freedom of expression than any company in the Index.
- Twitter improved its disclosure of how it responds to government requests to remove content and restrict accounts.
- Twitter disclosed ways for users to opt out of targeted advertising, which indicates that targeted advertising is on by default. In a setback for user privacy, the company disclosed it no longer responds to "Do Not Track" signals from users asking the company not to track them across third-party websites.

Key Recommendations:

- **Institutionalize policy commitments to freedom of expression and privacy.** Twitter should demonstrate that it has institutionalized comments to respect users' digital rights by disclosing whether and how it is implementing policies such as employee training and human rights impact assessments.
- **Protect users' privacy.** The company should show a stronger commitment to protect users' privacy by not sharing users' information for targeted advertising unless they opt in. It should also commit to respect signals from users to not track them across third-party websites.
- **Disclose more comprehensive information about security policies and practices.** Twitter should improve its disclosure of its internal processes for keeping user data secure, including the company's policies for responding to data breaches.

Analysis

Twitter ranked fifth out of 12 internet and mobile ecosystem companies, disclosing less about its policies affecting privacy than most of its U.S. peers. The company's score improved in the 2018 Index due to improved public commitments to users' freedom of expression and greater clarity in its transparency reporting on content removal requests.[1] However, Twitter's privacy score declined due to a change in its privacy policy stating that the company no longer responds to "Do Not Track" signals, and a lack of clear examples about how it implements its process for responding to government or private requests for user information. In addition, U.S. law prevents companies from disclosing the exact number of government requests for stored and real-time user information they receive, which prevented Twitter from being fully transparent in that area.[2]

About Twitter, Inc.

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

Market Cap: USD 24.5 billion[3]
NYSE: TWTR
Domicile: United States
Website: http://twitter.com/

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index.-For Twitter's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/twitter.
[2] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.
[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/TWTR:US.

Governance 46%

Twitter ranked fifth in the Governance category, scoring lower than most U.S. internet and mobile ecosystem companies evaluated, despite some notable improvements. The company strengthened its public commitment to respect users' freedom of expression and privacy (G1), improved its disclosure of senior-level oversight over these issues (G2), and disclosed a commitment to conduct human rights risk assessments when launching new products or entering into new markets (G4). While it disclosed that it regularly engages with a range of stakeholders on freedom of expression and privacy issues (G5), Twitter is not a member of a multi-stakeholder initiative like the Global Network Initiative (GNI), whose members not only make commitments but also undergo independent assessments to verify whether they have implemented and institutionalized them. As a result, Twitter's disclosure in the Governance category suffered compared to several of its other U.S.-based peers.

Freedom of Expression 61%

Twitter disclosed more than any of its peers about policies affecting freedom of expression.

Content and account restrictions: Twitter disclosed more than any other internet and mobile ecosystem company about its process for terms of service enforcement (F3, F4, F8). It disclosed more than most other companies about why it may restrict content or accounts (F3). It was one of only four companies, including Facebook, Microsoft, and Google, to disclose any data about its terms of service enforcement, reporting the number of accounts it restricted due to terrorist content and from legal requests to remove content or restrict accounts for violating Twitter's rules (F4). However, the data did not include all of the actions the company might take to enforce its rules.

Content and account restriction requests: Twitter disclosed less than Google and Oath about how it handles government and private requests to restrict content or accounts (F5-F7). It disclosed more data about government requests to restrict content or accounts than most of its U.S. peers (F6), and it provided more data than any other company about private requests to restrict content or accounts (F7).

Identity policy: Twitter and Microsoft were the only two internet and mobile ecosystem companies that disclosed that they do not require users to verify their identity with a government-issued ID or other information tied to their offline identity (F11).[4]

Privacy 53%

Twitter disclosed less than Google, Microsoft, Apple, and Oath about policies affecting users' privacy, but more than Facebook.

Handling of user information: Twitter offered more information than all other internet and mobile ecosystem companies about how it handles user information, but still fell short of Index benchmarks (P3-P9). It clearly disclosed what types of user information it collects (P3), but was less clear about what information it shares and with whom (P4). It disclosed more than any other company about how long it retains user information (P6), but disclosed little about whether users could access the information the company holds about them (P8). The company provides users with options for controlling how their information is collected for targeted advertising, suggesting targeted advertising is on by default (P7). Twitter's revised privacy policy made its practices of tracking users across third-party websites less clear (P9).[5] The company also disclosed it no longer respects "Do Not Track" (DNT) signals (P9).

Requests for user information: Twitter disclosed more than most of its peers, apart from Microsoft and Google, about how it handles government and private requests to hand over use data (P10-P12). Like most companies, it clearly disclosed its processes for responding to government requests for user information, but not for private requests it received (P10). It tied with Facebook for disclosing the most data on government and private requests for user information it received (P11).

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

[4] "Guidelines for Law Enforcement," Twitter Help Center, accessed March 13, 2017, https://help.twitter.com/articles/41949?lang=en.
[5] "Privacy Policy," Twitter, June 18, 2017, https://twitter.com/content/twitter-com/legal/en/privacy.html.

● Internet and Mobile Ecosystem Companies

Yandex N. V.

RANK	SCORE	DIFFERENCE FROM 2017
9	26%	0.00

SERVICES EVALUATED

- Yandex Mail (Email)
- Yandex Search (Search engine)
- Yandex Disk (Cloud service)

RANK AMONG 12 INTERNET AND MOBILE ECOSYSTEM COMPANIES

Key Findings:

- Yandex disclosed little about policies affecting users' freedom of expression and privacy, but more than Mail.Ru, the other Russian internet company evaluated.
- Yandex disclosed almost nothing about how it handles government demands to remove content or to hand over user data, although it is not illegal to disclose at least some information about its processes for responding to these types of requests.
- The company lacked clear disclosure of options users have to control what information the company collects and shares, and whether and how it tracks users across the internet using cookies, widgets, or other tracking tools.

Key Recommendations:

- **Make a clear commitment to human rights.** The company should express a clear commitment to freedom of expression and privacy as human rights, as there are no legal obstacles preventing the company from doing so.
- **Be transparent about external requests.** The company should disclose information about its handling of government requests to remove content and for user information, and indicate where laws may hinder full transparency.
- **Clarify handling of user information.** The company should improve disclosure of its handling of user data, including how long it retains it, and whether and how it tracks users across the internet.

Analysis

Yandex ranked ninth out of the 12 internet and mobile ecosystem companies evaluated, disclosing little about its policies and practices affecting freedom of expression and privacy. The company made no substantive improvements in the 2018 Index.[1] Notably, Yandex continued to disclose more than Mail.Ru about policies related to users' privacy.[2] While Yandex operates in an increasingly restrictive internet environment that discourages companies from publicly committing to protect human rights,[3] the company could still be more transparent about key policies affecting users' freedom of expression and privacy. It could disclose more about its processes for handling government and private demands to restrict content or to hand over user information, as there are no legal obstacles preventing the company from doing so. Yandex could also improve its commitments to users' privacy by clarifying its handling of user information, and giving users clear options to control what information the company collects and shares, and for how long it retains it, so that people can better understand the privacy, security, and human rights risks associated with Yandex services.

About Yandex N.V.

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

Market Cap: USD 13.9 billion[4]
NasdaqGS: YNDX
Domicile: Russia
Website: https://www.yandex.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Yandex's performance in the 2017 Index: see https://rankingdigitalrights.org/index2017/companies/yandex/.
[2] "Russian internet companies can do better despite tough legal environment," The 2017 Ranking Digital Rights Corporate Accountability Index, March 2017, https://rankingdigitalrights.org/index2017/findings/russia/.
[3] Freedom on the Net," (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/russia.

Governance 7%

Yandex scored poorly in the Governance category, ranking among the lowest internet and mobile ecosystem companies evaluated, but tying with Mail.Ru. The company received credit on three of the six indicators in this category. It disclosed a whistleblowing mechanism for reporting violations to privacy-related issues (G3), and published information about the impact of Russian law on user privacy (G4). Yandex also disclosed limited information about a grievance mechanism for users to file complaints about content removed for copyright violations, but not about content removed for terms of service violations (G6).

Freedom of Expression 21%

Yandex ranked tenth out of the 12 internet and mobile ecosystem companies evaluated in the Freedom of Expression category, disclosing less than Mail.Ru and most other companies.

Content and account restrictions: Yandex disclosed little about how it enforces its terms of service (F3, F4), although it had a similar level of disclosure as Apple. Yandex disclosed more about what the rules are and how they are enforced (F3) than actual data about the content or accounts the company restricted for violating its own rules (F4), and did not make clear whether it notifies users when content or their accounts have been restricted (F8).

Content and account restriction requests: Yandex also had weak disclosure about how it handles government and private requests to restrict content or accounts (F5, F6, F7), although it outperformed Mail.Ru, Tencent, Baidu, and Samsung on these indicators. The company disclosed limited information about its process for responding to government and private requests for content and account restrictions (F5), and published no data on the number of government requests it received or complied with (F6).

Identity policy: Yandex disclosed that it can ask users to confirm their offline identity, and may deny access to services to users who do not comply (F11). Internet service providers, telecommunications companies, and instant messaging services in Russia are legally required to verify the identities of their users, but it is unclear if the regulations apply to internet companies like Yandex.[5]

Privacy 36%

Yandex disclosed less than most of its peers about policies affecting users' privacy, but more than Tencent, Samsung, Mail.Ru, and Baidu.

Handling of user information: Yandex disclosed little about how it handles user information, but more than Mail.Ru. While the company disclosed some information about what types of user data it collects (P3), shares (P4), and for what purpose (P5), it revealed nothing about for how long it retains it (P6). While Yandex lacked clarity about what options users have to control what information the company collects and shares about them, it disclosed that users have options to control how their user information is used for targeted advertising (P7). However, Yandex failed to say whether and how it tracks users across the internet (P9), or if users can access all the information the company holds about them (P8).

Requests for user information: Yandex disclosed less than most of its peers but more than Mail.Ru about how it handles government and private requests for user information (P10-P12). It disclosed little about its process for responding to government or private requests for user information (P10) and supplied no data about requests it received or complied with (P11). However, since Russian authorities may have direct access to communications data, Russian companies may not be aware of the frequency or scope of user information accessed by authorities.[6]

Security: Yandex disclosed more than most internet and mobile ecosystem companies about policies and practices for keeping user information secure, lagging behind only Google and Apple (P13-P18). It disclosed a particularly strong bug bounty program (P14). Like most of its peers, Yandex provided no information about how it responds to data breaches (P15). The company, however, received the second-highest score after Google for its disclosure of it encryption policies (P16), disclosing that the transmission of users' communications is encrypted by default and with unique keys.

[4] Bloomberg Markets, accessed March 8, 2018, https://www.bloomberg.com/quote/YNDX:US.
[5] Law on Communications," No. 126-FZ (2003), as amended by Federal Law N 304-FZ in 2013, and "Amendments to Articles 10.1 and 15.4 of the Federal Law on Information, Information Technologies and Information Protection," No. 241-FZ (2017).
[6] Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's Back Door onto the Internet – Extract," *The Guardian*, September 8, 2015, http://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

Telecommunications Company

América Móvil , S.A.B. de C.V.

RANK: 5

SCORE: 21%

DIFFERENCE FROM 2017: ^ 0.39

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

OPERATING COMPANY EVALUATED

- **Telcel (Mexico)**

SERVICES EVALUATED

- **Pre-paid mobile**
- **Post-paid mobile**

Key Findings:

- América Móvil failed to disclose sufficient information about its policies and practices affecting users' freedom of expression and privacy.
- The company lacked disclosure about how it responds to government requests to shut down networks.
- The company did not clearly disclose how it handles government or private requests to block content or to hand over user information.

Key Recommendations:

- **Be transparent about policies affecting users' freedom of expression.** The company should be more transparent about how it responds to government requests to block content, restrict user accounts, and shut down networks.
- **Be transparent about external requests.** The company should disclose data about the number of government and private requests it receives to remove content and accounts and to hand over user information.
- **Disclose more about security practices.** The company should clearly communicate its handling of data breaches to users.

Analysis

América Móvil ranked fifth out of the 10 telecommunications companies evaluated, disclosing little about policies and practices affecting freedom of expression and privacy. The company slightly improved its disclosure of policies affecting users' freedom of expression in the 2018 Index.[1] Although Freedom House rates Mexico's internet environment as "Partly Free," the country's legal environment does not prevent the company from meeting basic benchmarks for transparency in key areas.[2] For instance, the company did not disclose its process for responding to government or private requests to block content or accounts, although no laws in Mexico prevent companies from doing so. In addition, although companies are required to report to the telecommunications authority the number of government requests received for real-time location tracking or access to user metadata, América Móvil did not publish this data.[3]

About América Móvil, S.A.B. de C.V.

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

Market Cap: USD 63.4 billion[4]
BMV: AMX L
Domicile: Mexico
Website: www.americamovil.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For América Móvil's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/americamovil.
[2] "Freedom on the Net," (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/mexico.
[3] "ACUERDO Mediante El Cual El Pleno Del Instituto Federal de Telecomunicaciones Expide Los Lineamientos de Colaboración En Materia de Seguridad Y Justicia Y Modifica El Plan Técnico Fundamental de Numeración, Publicado El 21 de Junio de 1996," (DOF - Diario Oficial de La Federación).
[4] Bloomberg Markets, accessed March 12, 2018, https://www.bloomberg.com/quote/AMXL:MM.

Governance 21%

América Móvil scored below most of its peers in the Governance category, but ahead of Bharti Airtel, Etisalat, Axiata, and Ooredoo. The company continued to lack clear disclosure of its commitments to human rights at the governance level, including whether it conducts human rights impact assessments (G4) or if it engages with a range of stakeholders on freedom of expression and privacy issues (G5). However, it disclosed more than most of its peers about remedy mechanisms addressing freedom of expression and privacy related complaints (G6). In Mexico companies are legally required to provide users with a complaint mechanism.[5]

Freedom of Expression 17%

América Móvil revealed little about its policies affecting freedom of expression, and less than Vodafone, AT&T, and Telefónica.

Content and account restriction requests: América Móvil was one of six telecommunications companies evaluated that offered no information about how it handles government or private requests to restrict content or accounts (F5-F7). There are no laws in Mexico preventing the company from being more transparent about how it handles such requests.

Network management and shutdowns: Telcel lacked disclosure about its network management policies (F9) and its approach to handling network shutdown requests from governments (F10). Despite committing to net neutrality, Telcel stated it offers zero rating for certain content on specific social networks and instant messaging services (F9).[6] Like most of its peers, the company disclosed no information about how it responds to government demands to shut down networks (F10).

Identity policy: Telcel's pre-paid contract asked users to provide their identification, although it was not clear if this is mandatory. In practice, it may be possible for users to purchase a pre-paid SIM card without providing identification, but the company failed to clarify this (F11).

Privacy 25%

América Móvil ranked fifth out of the 10 telecommunications companies evaluated in the Privacy category, ranking behind AT&T, Orange, and several other companies.

Handling of user information: Telcel disclosed less about how it handles user information than AT&T, Vodafone UK, and Telefónica Spain, but more than most other telecommunications companies evaluated (P3-P8). It disclosed little about what types of user information it collects (P3), shares (P4), and its reasons for doing so (P5). Like most of its peers, Telcel disclosed nothing about how long it retains user information (P6), although no law prohibits the company from doing so. It disclosed little about options users have to control what information is collected, including for targeted advertising (P7).

Requests for user information: Like most telecommunications companies, América Móvil provided almost no information about how it handles government and private requests for user information (P10), and failed to disclose whether it informs users when their information is requested (P12). The company did not publish any data about such requests (P11), despite being required by law to report the number of government requests for real-time location tracking or user metadata to the country's telecommunications authority.

Security: Telcel did not provide as much information about its security policies as Vodafone UK, AT&T, and Telefónica Spain, but was on par with Airtel India and Orange France (P13-P18). Telcel failed to disclose any information about how it addresses security vulnerabilities, including if it offers a bug bounty program for security researchers to submit vulnerabilities (P14). Like most companies in the Index, Telcel disclosed nothing about its policies for addressing data breaches (P15). Companies in Mexico are legally required to notify users only if the data breach "significantly affects" their rights, however the company does not disclose this information to users.[7]

[5] Ley Federal de Telecomunicaciones y Radiofusión, Última reforma publicada DOF 31-10-2017.
[6] "Política de Uso de Redes Sociales," *Telcel*, accessed March 12, 2018, https://www.telcel.com/mundo_telcel/quienes-somos/corporativo/redes-sociales.
[7] "Ley Federal de Protección de Datos Personales En Posesión de Los Particulares," Article 20 (2010).

Telecommunications Company

AT&T, Inc.

RANK: 2

SCORE: 49%

DIFFERENCE FROM 2017: ^ 0.72

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

OPERATING COMPANY EVALUATED

- **Telcel (Mexico)**

SERVICES EVALUATED

- **Pre-paid mobile**
- **Post-paid mobile**
- **Fixed-line broadband**

Key Findings:

- AT&T ranked second among telecommunications companies after Vodafone, disclosing more about policies affecting freedom of expression and privacy than most of its peers.
- The company did not clearly commit to engage with stakeholders about digital rights issues, unlike its European peers.
- AT&T disclosed more than any other telecommunications company about policies affecting users' privacy, but it could do more to explain what it does to keep user information secure.

Key Recommendations:

- **Engage with stakeholders on digital rights issues.** The company should join the Global Network Initiative (GNI) to better address the human rights risks of diverse user groups.
- **Be transparent about handling of user information.** The company should clearly disclose its practices around handling user information and give users more control over their own data.
- **Clearly communicate security practices.** The company should clearly communicate to users how it handles data breaches.

Analysis

AT&T received the second-highest score among telecommunications companies, after Vodafone.[1] The company made some improvements to policies affecting users' freedom of expression by clarifying its processes for handling government network shutdown demands, and strengthened its commitments to users' privacy by disclosing how users can obtain the data the company holds on them. However, AT&T's score in the Governance category declined due to its failure to join the Global Network Initiative (GNI) after the Telecommunications Industry Dialogue became inactive in March 2017. Despite positive steps in some areas, the company should take additional steps to ensure transparency of its network management policies and practices. AT&T should also give users greater control over their own data and disclose more about its security policies and practices. In addition, the company could disclose more about how it handles government and private requests to hand over user data. U.S. law prohibits companies from disclosing exact numbers of government requests for stored and real-time user information they receive, which prevented AT&T from being fully transparent in that area.[2]

About AT&T, Inc.

AT&T, Inc. provides telecommunications services in the United States and in Mexico, offering data and voice services to approximately 152 million wireless subscribers.[3]

Market Cap: USD 254.0 billion[4]
NYSE: T
Domicile: United States
Website: www.att.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. See AT&T's performance in the 2017 Index: https://rankingdigitalrights.org/index2017/companies/att.
[2] "USA FREEDOM Act of 2015," Pub. L. No. 114–23 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048.
[3] "3Q 2017 AT&T by the Numbers" (AT&T, 2017), https://www.att.com/Common/about_us/pdf/att_btn.pdf.
[4] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/T:US.

Governance 61%

AT&T ranked fourth in the Governance category among telecommunications companies, disclosing less than Vodafone, Telefónica, and Orange about how commitments to users' freedom of expression and privacy are institutionalized within the company. AT&T publicly committed to respect human rights, including freedom of expression and privacy (G1), and it provided evidence of senior-level oversight over these issues (G2). It also disclosed some information on its grievance and remedy mechanisms (G6). However, the company's overall score in this category declined due to a change in the company's public commitment to engage with stakeholders (G5). As of March 2017, the Telecommunications Industry Dialogue ceased to be active, and many of its members have joined GNI. However, AT&T did not join GNI, which resulted in a score decline.

Freedom of Expression 41%

AT&T earned the second-highest freedom of expression score among telecommunications companies, after Vodafone.

Content and account restriction requests: AT&T was one of only four telecommunications companies to receive any credit for disclosing information about its handling of government and private requests to restrict content or accounts (F5-F7). Notably, AT&T was one of three telecommunications companies to receive any credit for publishing data on government requests to restrict content or user accounts (F6), but it did not disclose any data about private requests (F7).

Network management and shutdowns: AT&T disclosed less information than Vodafone about its policies related to network management and shutdowns. While the company revealed reasons it may engage in network management practices, it did not commit not to engage in content blocking or prioritization practices (F9). AT&T clarified that it would report the number of government requests to shut down its networks if it received such requests (F10).

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

Privacy 49%

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

Handling of user information: AT&T disclosed more than all other telecommunications companies about how it handles user information (P3-P8). Still, it did not fully disclose what types of user information it collects (P3), shares (P4), and why (P5). The company revealed even less information about how long it retains user information (P6), although it and Vodafone were the only two telecommunications companies evaluated to score any points on this indicator. The company improved its disclosure regarding the options users have to access their own user data (P8). While options to download a copy of their data had already been available for AT&T's post-paid mobile users, the company disclosed additional options for pre-paid mobile and fixed-line broadband users to access their data.

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

Security: AT&T ranked second after Vodafone for disclosure of its security policies (P13-P18). It was the only one of its peers to receive full credit for disclosure of its internal processes for ensuring that user data is secure (P13). While AT&T was one of only four companies in the entire Index to reveal any information about how it handles data breaches, its disclosure still fell short (P15).

Telecommunications Company

Axiata Group Berhad

RANK: 8

SCORE: 14%

DIFFERENCE FROM 2017: 0.00

OPERATING COMPANY EVALUATED
- **Celcom (Malaysia)**

SERVICES EVALUATED
- **Pre-paid mobile**
- **Post-paid mobile**

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- Axiata was one of the lowest-scoring telecommunications companies in the Index, disclosing limited information on policies affecting freedom of expression and privacy.
- Axiata disclosed no information about its processes for responding to government or private requests to block content or user accounts or to hand over user information, although there are no legal obstacles preventing the company from disclosing some information about how it handles these types of requests.
- Axiata disclosed minimal information about its network management policies and practices, or how it handles government demands to shut down networks.

Key Recommendations:

- **Be more transparent about external requests.** Axiata should disclose information about its processes for responding to government and private requests to block content and accounts and to hand over user information.
- **Improve disclosure about network shutdowns.** Axiata should disclose more about how it handles government orders to shutdown networks, including making a clear commitment to push back against these types of demands.
- **Communicate more clearly about security.** Axiata should disclose information about its processes for keeping user information secure, including how it responds to data breaches.

Analysis

Axiata ranked eighth out of 10 telecommunications companies evaluated, disclosing less than most of its peers about policies and practices affecting freedom of expression and privacy. It made no substantive improvements in the 2018 Index.[1] The company operates in a challenging regulatory environment: the 2017 *Freedom on the Net* report by Freedom House rated Malaysia's internet environment as "Partly Free,"[2] and Celcom, Axiata's operating company in Malaysia, must comply with directives from the Malaysian Communications and Multimedia Commission (MCMC) and other authorities, many of which are not publicly available. However, there are no laws preventing Celcom from making basic commitments to respect freedom of expression and privacy rights, nor are there any legal obstacles preventing Axiata from improving its disclosure of how it handles user information.[3] Axiata could also be more transparent about how it handles government and private requests to hand over user information. While Malaysia's Official Secrets Act may prohibit some disclosure of government requests, nothing prevents Celcom from publishing at least some information about third-party requests for user information.[4]

About Axiata Group Berhad

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

Market Cap: USD 12.9 billion[6]
KLSE: AXIATA
Domicile: Malaysia
Website: https://www.axiata.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Axiata's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/axiata.
[2] "Freedom on the Net," (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/malaysia.

Governance 5%

Axiata received the second-lowest score of all companies evaluated in the Governance category, ahead of only Ooredoo. It received some credit on just two of the six indicators in this category. It disclosed that its board of directors has oversight over privacy issues (G2), and offered some information about ways users can submit privacy-related grievances (G6).[7]

Freedom of Expression 12%

Axiata received the second-lowest freedom of expression score among telecommunications companies, disclosing more about these policies and practices than only Bharti Airtel.

Content and account restriction requests: Like most of its peers, Axiata lacked clear disclosure of how it handles government and private requests to block content or accounts (F5-F7). It disclosed nothing about its process for responding to these types of requests (F5) nor did it publish any data about the number of these types of requests it receives or with which it complies (F6, F7).

Network management and shutdowns: Like most telecommunications companies evaluated, Celcom provided insufficient information about its network management and shutdown policies (F9, F10). It disclosed that it may block or delay certain types of traffic and applications (F9), but had minimal disclosure of why it may shut down access to the network for a user or group of users (F10).

Identity policy: Celcom disclosed that pre-paid mobile users must provide identification (F11), in accordance with Malaysian law.[8]

Privacy 18%

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

Handling of user information: Celcom provided more information than MTN South Africa, Etisalat UAE, and Ooredoo Qatar about how it handles user information (P3-P8), but its disclosure of what information it collects (P3), shares (P4), and why (P5) still fell short. Like most of its peers other than AT&T and Vodafone UK, Celcom provided no information about how long it retains user information (P6). It also offered users no information about options to control what information the company collects about them (P7), or options to obtain the information the company holds on them (P8). Malaysian law does not prevent companies from fully disclosing the information addressed in these indicators.

Requests for user information: Axiata was among three other telecommunications companies, including Etisalat and Ooredoo, to disclose nothing about how it handles requests from governments and private parties to hand over user information (P10-P12). It did not reveal any information about its processes for responding to these types of requests for user information, nor did it publish any data on the volume and nature of these requests it receives or complies with (P10, P11). It also did not commit to notify users if their information is requested (P12). There are no laws preventing the company from being more transparent about these processes.

Security: Celcom disclosed little about its security policies, scoring better than only MTN South Africa, Etisalat UAE, and Ooredoo Qatar on these indicators (P13-P18). Its disclosure about conducting security audits improved, but its disclosure of its policies for monitoring employee access to user information was less transparent than in the 2017 Index. The company did not disclose policies for addressing security vulnerabilities (P14) or for responding to data breaches (P15).

[3] Personal Data Protection Act 2010," Act 709 (2010), http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf.
[4] "Official Secrets Act 1972," Act 88 (1972), http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%2088.pdf.
[5] "Key Highlights," *Axiata Group Berhad*, accessed March 13, 2018, https://www.axiata.com/corporate/key-highlights/.
[6] Bloomberg Markets, accessed February 26, 2018, https://www.bloomberg.com/quote/AXIATA:MK.
[7] "Privacy Policy," Celcom, August 1, 2013, https://www.celcom.com.my/legal/privacy-policy.
[8] The "Prepaid Registration Exercise in Malaysia" (Malaysian Communications and Multimedia Commission), directive requires telecommunications companies to register pre-paid SIM cards with a user's identity card or passport, accessed March 13, 2018, https://www.mcmc.gov.my/skmmgovmy/files/attachments/Info-updated%204July06.pdf.

Telecommunications Company

Bharti Airtel Limited

OPERATING COMPANY EVALUATED
- **Airtel India**

SERVICES EVALUATED
- **Pre-paid mobile**
- **Post-paid mobile**
- **Fixed-line broadband**

RANK
7

SCORE
15%

DIFFERENCE FROM 2017
^ 0.46

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- Bharti Airtel disclosed less about policies and practices affecting freedom of expression and privacy than most other telecommunications companies evaluated.
- It disclosed almost no information about its policies for responding to network shutdown demands from the Indian government, despite the increasing number of these types of requests and the significant human rights risks they pose.
- The company disclosed more than most of its peers about its grievance and remedy mechanisms, since Indian law requires companies to offer users redress.

Key Recommendations:

- **Disclose more about network shutdowns.** Bharti Airtel should disclose information about its policies and practices for handling government demands to shut down networks, and commit to push back on such requests.
- **Be transparent about external requests.** The company should disclose information about its processes for responding to government and private requests to block content or restrict accounts and to hand over user information.
- **Clarify security policies.** Bharti Airtel should disclose more about its security policies and practices, including its processes for responding to data breaches.

Analysis

Bharti Airtel ranked seventh out of the 10 telecommunications companies evaluated, disclosing less than most of its peers about policies and practices affecting freedom of expression and privacy.[1] The company made a slight improvement to its privacy commitments by disclosing employee training on security practices and that it monitors employee access to user information. Notably, Bharti Airtel received one of the highest scores in the Index for its grievance and remedy mechanisms (G6), as Indian law requires service providers to have redress mechanisms in place.[2] However, the company continued to disclose less than any other telecommunications company in the Index about policies affecting freedom of expression. Freedom House rates the internet environment in India as "Partly Free," noting a sharp increase in the number of government orders to shutdown networks.[3] Still, the company disclosed little about its policies for responding to these types of government demands. While Indian law prevents companies from disclosing information about specific government content restriction and shutdown orders, there are no legal obstacles preventing companies from disclosing policies for responding to these requests or from having a policy of notifying users about these actions.

About Bharti Airtel Limited

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

Market Cap: USD 26.1 billion[4]
BSE: 532454
Domicile: India
Website: www.airtel.in

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Bharti Airtel's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/bhartiairtel.
[2] "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" (Ministry of Communications and Information Technology, April 11, 2011), http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
[3] "Freedom on the Net" (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/india.

Governance 17%

Bharti Airtel scored poorly in the Governance category, placing in the bottom half of all telecommunications companies evaluated. While it has a corporate social responsibility program that stresses the importance of a "responsible business approach" addressing "every dimension of how business operates in the social, cultural, and economic environment,"[5] the company demonstrated weak commitments to users' freedom of expression and privacy rights. While scoring less than most other telecommunications companies on all governance indicators, it outperformed most of its peers on disclosure of grievance and remedy mechanisms (G6). Notably, Bharti Airtel tied for second place with Vodafone for grievance and remedy mechanisms (G6), as Indian law requires service providers to have grievance officers and redress mechanisms in place.[6]

Freedom of Expression 9%

Bharti Airtel disclosed less than any other telecommunications company about policies affecting freedom of expression.

Content and account restriction requests: Like most of its peers, Bharti Airtel disclosed nothing about how it handles and complies with government and private requests to restrict content or accounts (F5-F7). Indian law forbids disclosure of specific government orders to block content,[7] but nothing prevents companies from disclosing processes for handling these types of requests, or from having a clear policy of notifying users when they restrict or block content that users publish, transmit, or attempt to access (F8).

Network management and shutdowns: Airtel India disclosed little information about its network management policies (F9) or about its policies and practices related to network shutdowns (F10). The company lost points for disclosure of its network management practices, since its previously disclosed zero rating program was no longer in effect (F9). While Indian law prevents companies from disclosing information about specific government shutdown orders,[8] there is no legal obstacle to disclosing company policies for evaluating and responding to shutdown requests, or from having a policy to notify users about shutdowns.

Identity policy: Airtel India disclosed that it requires pre-paid mobile users to provide government-issued identification (F11), as required by law.[9]

Privacy 18%

Bharti Airtel disclosed little about policies affecting users' privacy, disclosing more than only MTN, Etisalat, and Ooredoo, the lowest-scoring companies in this category.

Handling of user information: Airtel India disclosed less than most other telecommunications companies about how it handles user information, but more than MTN South Africa, Etisalat UAE, and Ooredoo Qatar (P3-P8). It disclosed some information about what types of user information it collects, shares, and for what purpose (P3, P4, P5), but nothing about how long it retains this information (P6). The company also failed to disclose whether it enables users to control what information about them is collected and shared, or if users can obtain the information the company holds about them (P7, P8).

Requests for user information: Like most other telecommunications companies, Bharti Airtel disclosed little about how it handles government and private requests for user information (P10-P11). Indian law prevents companies from publishing data on government requests for user information but does not prevent them from disclosing their processes for responding to these requests.

Security: Airtel India scored above the telecommunications company average on these indicators, on par with América Móvil's Telcel and Orange France (P13-P18). The company slightly improved its disclosure of policies limiting employee access to user data (P13), however it offered no information about its policies for addressing security vulnerabilities (P14) or for responding to data breaches (P15).

[4] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/BHARTI:IN.
[5] "Sustainability," Airtel India, accessed March 14, 2018, http://www.airtel.in/sustainability-file/home.html.
[6] "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" (Ministry of Communications and Information Technology, April 11, 2011), http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511[1].pdf.
[7] "Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009" The Centre for Internet & Society, http://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009.
[8] "License Agreement for Provision of Internet Services" (Government of India Ministry of Communications & IT), accessed March 14, 2018, "License Agreement for Provision of United Access Services after Migration from CMTS" (Government of India Ministry of Communications & IT, December 3, 2009), and "License Agreement for Unified License" (Government of India Ministry of Communications & IT), accessed March 14, 2018.
[9] "Subscriber Verification," Department of Telecommunications, accessed March 14, 2018.

Telecommunications Company

Etisalat Group

RANK	SCORE	DIFFERENCE FROM 2017
9	8%	^ 0.52

OPERATING COMPANY EVALUATED
- **Etisalat UAE**

SERVICES EVALUATED
- **Pre-paid mobile**
- **Post-paid mobile**
- **Fixed-line broadband**

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- Etisalat was one of the lowest-scoring telecommunications companies in the Index, disclosing almost nothing about policies and practices affecting users' freedom of expression and privacy.
- The company failed to disclose even basic information about its privacy policies, including which policy applied to which service.
- While slightly improving its disclosure of its security policies, Etisalat disclosed almost nothing about policies affecting users' privacy, including what user information it collects, shares, or for what purpose, or how it handles government and private requests to hand over user information.

Key Recommendations:

- **Improve privacy policy disclosure.** The company should clarify which privacy policies apply to different services, and be more transparent about how it handles user information.
- **Be transparent about private requests.** The company should disclose its processes for responding to private requests to block content or accounts and to hand over user data, and regularly publish data about these requests.
- **Improve redress.** The company should improve its grievance mechanisms by disclosing that its process for receiving complaints includes complaints related to freedom of expression and privacy, and providing clear remedies for these types of complaints.

Analysis

Etisalat ranked ninth out of the 10 telecommunications companies, disclosing almost nothing about policies and practices affecting freedom of expression and privacy.[1] Etisalat is a majority state-owned company,[2] operating in a political and regulatory environment that restricts expression online.[3] While companies in the UAE are discouraged from making public commitments to human rights, Etisalat could still be more transparent about basic policies affecting users' freedom of expression and privacy. For instance, it could clarify which privacy policies apply to different services. It could also provide more information about its security policies, as there is no law prohibiting companies from disclosing their processes for responding to data breaches. Given that the company is majority state-owned and that the overall operating environment discourages transparency, it is unlikely Etisalat would disclose information about government requests to block content or to hand over user information. However, Etisalat could disclose its policies for responding to private requests.

About Etisalat Group

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

Market Cap: USD 41.2 billion[4]
ADX: ETISALAT
Domicile: United Arab Emirates (UAE)
Website: www.etisalat.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Etisalat's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/etisalat.
[2] "Investor Relations - Investor Relations," Etisalat, accessed March 15, 2018, http://www.etisalat.com/en/ir/corporateinfo/overview.jsp.
[3] "Freedom on the Net" (Freedom House, November 2017), https://freedomhouse.org/report/freedom-net/2017/united-arab-emirates.
[4] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/ETISALAT:UH.

Governance 7%

Etisalat performed poorly in the Governance category, scoring higher than only Axiata and Ooredoo. Etisalat provided no formal commitment to respect users' freedom of expression and privacy as human rights (G1), and disclosed no senior-level oversight over these issues (G2). The company revealed no evidence of a human rights due diligence process (G4), or of engaging with stakeholders on freedom of expression or privacy issues (G5). It received some credit for disclosing a grievance and remedy mechanism, though the company did not explicitly state that this process includes complaints relating to free expression or privacy (G6).

Freedom of Expression 15%

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

Content and account restriction requests: Like most telecommunications companies, Etisalat provided almost no information about how it handles government or private requests to block content or restrict accounts (F5-F7). Likewise, Etisalat did not publish any data on the number of such requests it received or with which it complied (F6, F7). While it is a criminal offense to not comply with government blocking orders,[5] there is no law prohibiting Etisalat from disclosing its processes for handling or compliance rates with either government or private content-blocking requests.

Network management and shutdowns: Etisalat UAE was among the lowest-scoring companies on these indicators, though it offered slightly more disclosure than Ooredoo Qatar (F9-F10). The company failed to disclose any information about its network management policies (F9) and disclosed almost nothing about its policies for responding to government orders to shutdown networks (F10).

Identity policy: Etisalat UAE disclosed that it requires pre-paid mobile service users to provide government-issued identification (F11), as it is mandated for all mobile phone service subscribers in the UAE.[6]

Privacy 4%

Etisalat received the second-lowest privacy score of all telecommunications companies evaluated, disclosing slightly more than Qatar-based telecommunications operator, Ooredoo.

Handling of user information: Etisalat UAE disclosed almost nothing about how it handles user information, scoring better than only Ooredoo Qatar on these indicators (P3-P8). The company's privacy policy referred only to the Etisalat UAE website and online services with no indication of whether this policy applies to mobile or fixed-line broadband services. It therefore received no credit on indicators addressing company disclosure of what types of user information it collects, for what purpose, and for how long it retains it (P3, P5, P6). The company did not disclose options users have to control what information it collects and shares about them (P7). The company did, however, disclose that it shares user information with authorities if legally required and in cases of national security (P4).

Requests for user information: Etisalat provided no information about how it handles government or private requests for user information, making it one of three companies, along with Ooredoo and Axiata, that received no credit on these indicators (P10, P11, P12). It provided no information about its process for responding to these types of requests (P10), or whether it notifies users when their information is requested (P12). The company also did not publish any data on the number of requests it received for user information (P11). However, Etisalat's operating license requires it to install equipment allowing authorities to access the network, so the company may not be aware when government authorities access user information.[7] Still, there is no law specifically prohibiting Etisalat from disclosing its policy for responding to user information requests that come through private processes.

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

[5] "Federal Decree-Law No. (5) of 2012 on Combatting Cybercrimes" (2012), http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf.
[6] "TRA Links Mobile Registration with 'ID Card,'" Emirates Identity Authority, February 9, 2015.
[7] "Public Telecommunications License No. 1/2006" Telecommunications Regulatory Authority, accessed March 15, 2018.

Telecommunications Company

MTN Group Limited

OPERATING COMPANY EVALUATED
- **MTN South Africa**

SERVICES EVALUATED
- **Pre-paid mobile**
- **Post-paid mobile**

RANK
6

SCORE
16%

DIFFERENCE FROM 2017
^ 0.09

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- MTN disclosed less about policies and practices affecting freedom of expression and privacy than most of its peers.
- While it completed its first human rights impact assessment evaluating risks to users' freedom of expression and privacy, MTN still lacked transparency about key policies affecting these rights, including how it handles government requests to shut down networks and to hand over user information.
- MTN disclosed almost nothing about how it handles user information, including what it collects, shares, and for what purpose, as well as what steps it takes to keep user information secure.

Key Recommendations:

- **Be more transparent about external requests affecting user rights.** MTN should disclose information about government and private requests to restrict content or accounts, and about private requests for user information.
- **Improve disclosure about network shutdowns.** MTN should disclose more information about how the company handles government network shutdowns, including making a clear commitment to push back against these types of requests.
- **Do more to protect privacy and security.** MTN should be more transparent about how it handles user information, including how it keeps user information secure.

Analysis

MTN ranked sixth out of the 10 telecommunications companies evaluated, disclosing little about policies and practices affecting freedom of expression and privacy.[1] In 2017, the company conducted its first human rights impact assessment evaluating freedom of expression and privacy risks associated with its products and services, resulting in an improved governance score in the 2018 Index. However, MTN's privacy score declined due to less clear disclosure of how it responds to government requests for user information. While South African law prevents MTN South Africa from disclosing information about government requests for user information, MTN at the group level could still be much more transparent about many of its policies and practices that affect users' freedom of expression and privacy.

About MTN Group Limited

MTN Group Limited is a telecommunications company that serves markets in 24 countries in Africa and the Middle East.[2] It offers voice and data services, and business services, such as cloud, infrastructure, network, software, and enterprise mobility.

Market Cap: USD 21.3 billion[3]
JSE: MTN
Domicile: South Africa
Website: www.mtn.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index.-For MTN's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/mtn.
[2] "Where We Are," MTN Group, accessed March 16, 2018, https://www.mtn.com/en/mtn-group/about-us/our-story/Pages/where-we-are.aspx.
[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/MTN:SJ.
[4] " Devin Coldewey, "WTF Is Zero Rating?," *TechCrunch*, April 16, 2017, https://social.techcrunch.com/2017/04/16/wtf-is-zero-rating/.
[5] "Annual Sustainability Report for the Year Ended 31 December 2016" (MTN Group Limited, 2017), https://www.mtn.com/MTN%20Service%20Detail%20Report%20archive/MTN%20Group%20Sustainability%20Report%202016.pdf.

Governance 38%

MTN received the fifth-best governance score among telecommunications companies. It improved its governance score in the 2018 Index by disclosing it conducted human rights due diligence on its products and services (G4). The company disclosed an explicit commitment to freedom of expression and privacy as human rights (G1), and evidence of senior leadership oversight within the company on these issues (G2). However, the company fell short on other governance indicators: it disclosed a whistleblower program, but only for reporting cases of corruption and fraud (G3). Likewise, it lacked clear disclosure of whether it engages with stakeholders representing people whose freedom of expression and privacy are directly impacted by the company's business (G5), or of a grievance and remedy mechanism allowing users to voice freedom of expression and privacy complaints (G6).

Freedom of Expression 12%

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

Content and account restriction requests: MTN was one of six telecommunications companies to disclose nothing about its process for handling government and private requests to block content or restrict user accounts (F5-F7). South African law does not prevent companies from disclosing information about how they handle these requests, nor does it prohibit them from publishing this data.

Network management and shutdowns: MTN South Africa disclosed little about its network management and shutdown policies, on par with Airtel India and América Móvil's Telcel (F9). The company disclosed a program enabling users to access Facebook without it counting towards their data cap, a practice known as "zero rating," but disclosed no additional information about its network management practices (F9).[4] MTN committed to notify users about network service disruptions when it is "safe and legal" to do so,[5] and provided an example of when it pushed back against a network shutdown request,[6] though it fell short of making a clear and unequivocal commitment to push back against all such requests (F10).

Identity policy: MTN South Africa did not disclose if it requires pre-paid mobile users to register their SIM card with the company using their government-issued identification. All mobile phone users in South Africa are legally required to do so (F11).[7]

Privacy 11%

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

Handling of user information: MTN South Africa disclosed less than most of its peers about its handling of user information (P3-P8). It provided just minimal information about what types of user information it collects and why (P3, P5), and no information about what information it shares (P4), or for how long it retains user information (P6). It also did not disclose any options for users to control what information the company collects and uses (P7), or options for users to obtain all of the information the company holds on them (P8).

Requests for user information: Like most telecommunications companies, MTN provided almost no information about how it handles government and private requests for user information (P10-P11). While the company previously provided information on how it carries out due diligence on government and private requests,[8] researchers were unable to locate such information in current company disclosure. Companies in South Africa are prohibited from publishing information about government requests for user information, including the fact that a request was made,[9] but nothing prevents them from fully disclosing how they handle private requests and the number of these requests they receive and comply with.

Security: MTN South Africa disclosed minimal information about its security policies, performing better than only Etisalat UAE and Ooredoo Qatar on these indicators (P13-P18). However, it was one of only two telecommunications companies (along with AT&T) to offer any disclosure on its processes for addressing security vulnerabilities (P14). Like most of its peers, MTN South Africa provided no information about its policies for responding in the event of a data breach (P15).

[6] "Annual Sustainability Report for the Year Ended 31 December 2015" (MTN Group Limited, 2016) https://www.mtn.com/MTN%20Service%20Detail%20Report%20archive/MTN_Group_Sustainabilty_Report_2015.pdf.
[7] "Regulation Of Interception Of Communications And Provision Of Communication-Related Information Act," Pub. L. No. Act No. 70 (2002).
[8] "Social and Ethics Report," MTN, March 28, 2013, http://www.mtn-investor.com/mtn_ar2012/gov-social.php.
[9] "Regulation Of Interception Of Communications And Provision Of Communication-Related Information Act," Pub. L. No. Act No. 70 (2002).

Telecommunications Company

Ooredoo Q.S.C.

RANK	SCORE	DIFFERENCE FROM 2017
10	5%	0.00

OPERATING COMPANY EVALUATED
- **Ooredoo Qatar**

SERVICES EVALUATED
- **Pre-paid mobile**
- **Post-paid mobile**
- **Fixed-line broadband**

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- Ooredoo was the lowest scoring telecommunications company in the Index, disclosing almost nothing about policies and practices affecting freedom of expression and privacy.
- The company failed to disclose sufficient information about its policies affecting users' freedom of expression, including its processes for blocking content or responding to government demands to shut down networks.
- It did not publish a privacy policy, making it impossible for users to understand what the company does with their information, including what it collects, shares, and why.

Key Recommendations:

- **Publish privacy policies.** Ooredoo should clearly disclose its privacy policies and ensure these policies are both easy to find and to understand.
- **Clarify content and access restrictions.** Ooredoo should be more transparent about its process for handling government and private requests to block content or restrict user accounts, and for handling government requests to shut down networks.
- **Improve redress.** The company should improve its grievance mechanisms by disclosing that its process for receiving complaints includes complaints related to freedom of expression and privacy, and providing clear remedies for these types of complaints.

Analysis

Ooredoo received the lowest score of all telecommunications companies, disclosing less about policies and practices affecting users' freedom of expression and privacy than any of its peers, including Etisalat, the UAE-based telecommunications company.[1] Ooredoo, which is majority owned by the government of Qatar, was one of four companies in the Index to make no improvements in the 2018 Index. While the political and regulatory environment in Qatar discourages companies from making public commitments to human rights,[2] the company could still be more transparent about basic policies affecting freedom of expression and privacy in a number of areas. For instance, it could make its privacy policies publicly available to users. It could also provide information about what steps it takes to keep user information secure, as there are no legal obstacles preventing the company from doing so. In 2016, Qatar passed its first comprehensive data privacy law requiring companies to notify the regulators and users in the event of a data breach, but the company does not disclose this information.[3]

About Ooredoo Q.S.C.

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

Market Cap: USD 8.6 billion[5]
DSM: ORDS
Domicile: Qatar
Website: https://www.ooredoo.qa/

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index.-For Ooredoo's performance in the 2017 Index: https://rankingdigitalrights.org/index2017/companies/ooredoo/.
[2] "Freedom of the Press 2017. Qatar Profile," (Freedom House, 2017), https://freedomhouse.org/report/freedom-press/2017/qatar.
[3] Tribune News Network, "New Law on Personal Data Protection," *Qatar Tribune*, November 4, 2016, http://www.qatar-tribune.com/news-details/id/31687.

Governance 2%

Ooredoo performed poorly in the Governance category, receiving the lowest score of all telecommunications companies. It did not make a public commitment to respect freedom of expression and privacy as human rights (G1), nor did it disclose having senior-level oversight over these issues within the company (G2). Although it disclosed a whistleblower policy, it did not mention if this policy pertains to freedom of expression or privacy issues (G3). It offered no evidence that it has any human rights due diligence processes in place (G4), or if it engages with stakeholders on freedom of expression or privacy issues (G5). Ooredoo disclosed some information about a grievance mechanism through which customers may submit complaints, but there was no additional information about its processes for receiving and responding to such grievances (G6).

Freedom of Expression 14%

Ooredoo disclosed little about policies affecting freedom of expression, receiving the third-lowest score among telecommunications companies, ahead of MTN, Axiata, and Bharti Airtel.

Content and account restriction requests: Ooredoo, like most of its peers, provided no information about its process for responding to government or private requests to block content or restrict users' accounts (F5), nor did it supply any data about the number of government or private requests to restrict content or accounts that it receives or complies with (F6, F7). There is no apparent legal barrier to supplying this information. The lack of disclosure is likely a result of Ooredoo being majority state-owned as well as from a general lack of transparency in the Qatari legal environment. Telecommunications companies in Qatar are legally required to comply with all judicial orders to block content,[6] though there is no law prohibiting Ooredoo from disclosing its processes for handling or compliance rates with either government or private content-blocking requests.

Network management and shutdowns: Ooredoo Qatar did not disclose any information about its network management policies (F9). Like most telecommunications companies, it disclosed little about its processes for handling government requests to shutdown its networks (F10).[7]

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

Privacy 0%

Ooredoo received the lowest privacy score of all telecommunications companies evaluated, as the company did not publish a privacy policy for pre- or post-paid mobile, or for fixed-line broadband services.

Handling of user information: Ooredoo Qatar was the only company in the entire Index to disclose nothing about what user information it collects, shares, retains, and its reasons for doing so (P3-P8). The company did not publish a privacy policy for the services evaluated.

Requests for user information: Ooredoo provided no information about how it handles government or private requests for user information, making it one of three companies, along with Etisalat and Axiata, that received no credit on these indicators (P10, P11, P12). It provided no information about its process for responding to these types of requests (P10), or whether it notifies users when their information is requested (P12). The company also did not publish any data on the number of requests it received for user information (P11). The lack of disclosure is likely a result of Ooredoo being majority state-owned as well as from a general lack of transparency in the Qatari legal environment. Still, there is no law specifically prohibiting Ooredoo from disclosing its policies for responding to user information requests that come through private processes.

Security: Ooredoo Qatar was the only company in the entire Index to disclose nothing about its policies and processes for keeping users' information secure (P13-P18). It did not disclose whether it has systems in place to monitor or limit employee access to user information (P13), nor did it provide any information about its processes for addressing security vulnerabilities or for handling data breaches (P14, P15).

[4] "Our Markets," Ooredoo Corporate, accessed March 15, 2018, http://ooredoo.com/en/who_we_are/our_markets/.
[5] Bloomberg Markets, Accessed February 13, 2018, https://www.bloomberg.com/quote/ORDS:UH.
[6] Peter Kovessy, "Qatar's Emir Signs New Cybercrime Legislation into Law," *Doha News*, September 16, 2014, https://dohanews.co/qatars-emir-signs-law-new-cybercrime-legislation/.
[7] General Terms and Conditions for Consumer Services," Ooredoo, accessed March 15, 2018, https://www.ooredoo.qa/portal/OoredooQatar/general-terms-and-conditions.

Telecommunications Company

Orange S.A.

RANK

4

SCORE

33%

DIFFERENCE FROM 2017

∧ 2.09

OPERATING COMPANY EVALUATED

- **Orange France**

SERVICES EVALUATED

- **Pre-paid mobile**
- **Post-paid mobile**
- **Fixed-line broadband**

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- Orange disclosed more about policies affecting users' freedom of expression and privacy than most telecommunications companies evaluated, but less than its European peers.
- The company improved its disclosure of how it handles network shutdown requests from governments, but lacked sufficient information about other policies affecting users' freedom of expression.
- Orange disclosed far less about how it handles user information than its European peers, and almost nothing about how it keeps user information secure.

Key Recommendations:

- **Improve grievance and remedy mechanisms.** Orange should improve its grievance mechanisms by providing clear procedures for users to directly submit complaints of violations to their freedom of expression or privacy rights.
- **Improve disclosure of external requests.** Orange should disclose more about how it responds to government and private requests to block content or restrict user accounts.
- **Clarify security practices.** Orange should disclose more about what it does to protect user data and how it responds in cases of data breaches.

Analysis

Orange ranked fourth among the 10 telecommunications companies evaluated, disclosing less about its policies and practices affecting freedom of expression and privacy than Vodafone, AT&T, and Telefónica.[1] The company disclosed a strong commitment to freedom of expression and privacy as human rights, and as a full member of the Global Network Initiative (GNI) since March 2017, it now commits to engage with a range of stakeholders on freedom of expression and privacy issues. Orange made several positive changes in the 2018 Index, including clarifying a commitment to push back on government requests to shut down networks and improving its disclosure of options users have to obtain the information that Orange holds about them. Despite these steps, the company fell short of its European and GNI peers in key areas. It disclosed nothing about how it handles government requests to block content or restrict user accounts, and Orange France did not provide the same level of detail as Vodafone UK or Telefónica Spain about its handling of user information. The company also lacked disclosure of its internal security procedures for keeping user data secure.

About Orange S.A.

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

Market Cap: USD 45 billion[2]
ENXTPA: ORA
Domicile: France
Website: www.orange.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Orange's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/orange/.
[2] Bloomberg Markets, accessed February 22, 2018, https://www.bloomberg.com/quote/ORA:FP.

Governance 76%

Orange received the third-highest governance score among telecommunications companies, after Vodafone and Telefónica. Orange's governance score improved in the 2018 Index due to its joining the Global Network initiative (GNI) and to its improved clarity of its human rights due diligence practices. Notably, it earned the highest score among telecommunications companies for its human rights due diligence commitments (G4).[3] However, the company disclosed almost nothing about its grievance and remedy mechanisms (G6), tying with Ooredoo for the second-lowest score among telecommunications companies on this indicator.

Freedom of Expression 17%

Orange disclosed little about its policies affecting users' freedom of expression, lagging behind Vodafone, AT&T, and Telefónica in this category.

Content and account restriction requests: Unlike AT&T, Vodafone, and Telefónica, Orange disclosed no information about how it handles government and private requests to block websites, content, or user accounts (F5-F7). There are no legal obstacles preventing Orange from disclosing this information.

Network management and shutdowns: As in the 2017 Index, Orange France disclosed nothing about its network management practices (F9), making it one of three companies, along with Etisalat UAE and Ooredoo Qatar, to receive no credit on this indicator (F9). While it clarified a commitment to push back on government requests to shut down networks, the company still revealed little about its processes for responding to these requests, lagging behind Vodafone UK, AT&T, and Telefónica Spain on this indicator (F10).

Identity policy: Orange France requires pre-paid customers to provide a government-issued ID to activate a SIM card. This appears to be legally required in France.[4]

Privacy 29%

Orange failed to disclose sufficient information about policies affecting users' privacy, ranking fourth among telecommunications companies in this category, behind AT&T, Vodafone, and Telefónica.

Handling of user information: Orange France disclosed less information than Vodafone UK and AT&T about how it handles user information (P3-P8), but more than the rest of its peers. It did not disclose if targeted advertising is off by default, and provided only its fixed-broadband customers with a few options to control how their information is used for targeted advertising (P7). The company clarified that users can obtain a copy of the data that Orange France holds on them (P8), although it still did not indicate if this includes all of the public and private data it holds.

Requests for user information: Orange disclosed less than AT&T, Vodafone, and Telefónica about how it handles government and private requests for user information (P10, P11). While Orange provided some data on government requests for user information, it failed to provide data on such requests for a number of countries in which the company operates.[5] When national law prohibits the release of such data, Orange should specify the legal barrier to disclosure. Orange, like the rest of its peers, did not commit to notify users about government and private requests for their data (P12).

Security: Orange France disclosed less than Vodafone UK, AT&T, and Telefónica Spain about its security policies (P13-P18). The company disclosed some information about its internal mechanisms to keep user information secure (P13), but provided no information about what it does to address security vulnerabilities (P14), and disclosed nothing about its processes for responding to data breaches (P15). There are no legal obstacles preventing the company from disclosing how it handles security breaches.

[3] "Orange and Human Rights: 2016 Report" (Orange, November 2017), https://www.orange.com/en/content/download/45336/1348812/version/7/file/Report+2016+Orange+Human+Rights+DIGITAL-VA.pdf.
[4] "Code Des Postes et Des Communications Électroniques," Article R10-13 (2006), https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006466369.
[5] "Orange Transparency Report on Freedom of Expression and Privacy Protection: Year 2016" (Orange, 2017), https://www.orange.com/en/content/download/43262/1315009/version/2/file/2017%20RAPPORT%20DE%20TRANSPARENCE_20.06.2017_final_eng.pdf.

Telecommunications Company

Telefónica, S.A.

RANK

3

SCORE

41%

DIFFERENCE FROM 2017

^ 5.51

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

OPERATING COMPANY EVALUATED

- **Telefónica Spain**

SERVICES EVALUATED

- **Pre-paid mobile (Movistar)**
- **Post-paid mobile (Movistar)**
- **Fixed-line broadband (Movistar)**

Key Findings:

- Telefónica disclosed a strong commitment to respect human rights but was less transparent about policies affecting users' freedom of expression and privacy in practice.
- The company improved its disclosure of how it handles government requests to shutdown networks, block content, and hand over user information, but could still publish more data about its compliance with these types of requests.
- Telefónica lacked transparency about how it handles user information and what steps it takes to keep user information secure.

Key Recommendations:

- **Improve transparency reporting.** Telefónica should disclose more detailed data about its compliance with government and private requests to block content or accounts, and for user information.
- **Clarify handling of user information.** Telefónica should disclose what user information it shares and retains, and whether users can obtain the information the company holds on them.
- **Communicate more clearly about security.** Telefónica should clearly disclose how it keeps user information secure, including if it limits employee access to user information.

Analysis

Telefónica ranked third out of 10 telecommunications companies evaluated, after Vodafone and AT&T, and disclosed a strong commitment to protecting users' freedom of expression and privacy.[1] As a full member of the Global Network Initiative (GNI) since March 2017, the company now commits to engaging with a range of stakeholders on freedom of expression and privacy issues. The company made numerous improvements in the 2018 Index, including clarifying its process for handling government requests to shut down networks and providing more data about government requests for user data. Despite positive steps, the company could be more transparent about policies affecting users' freedom of expression by publishing more data about government and private requests it receives to block content or accounts, as there are no legal obstacles in its home market of Spain preventing the company from doing so. It could also improve its commitments to protect users' privacy by disclosing what user data it shares and with whom, and by providing greater clarity about what steps it takes to keep user information secure.

About Telefónica, S.A.

Telefónica, S.A. provides mobile, fixed-line broadband, and other services to more than 276 million mobile customers in Spain, Latin America, and internationally.[2]

Market Cap: USD 51.3 billion[3]
BME: TEF
Domicile: Spain
Website: https://www.telefonica.com/

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index.For Telefónica's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/telefonica.
[2] "Telefónica in Numbers - FY2016," Telefónica, accessed March 13, 2018, https://www.telefonica.com/documents/153952/141433988/Telefonica_in_numbers_FY2016.pdf/81ba0d34-c6da-9621-09b0-716d918cc0e5.
[3] Bloomberg Markets, accessed February 26, 2018, https://www.bloomberg.com/quote/TEF:SM.
[4] "Responsible Business Channel," Telefónica, accessed March 13, 2018, https://www.telefonica.com/en/web/about_telefonica/responsible-business-channel.

Governance 77%

Telefónica ranked second in the Governance category among telecommunications companies, after Vodafone. It significantly improved its disclosure of its public commitment to freedom of expression and privacy, resulting in increased scores in five of the six indicators in this category. The company improved its disclosure of senior-level oversight over freedom of expression and privacy issues within the company (G2), clarified that the company provides its employees with training on freedom of expression (G3), and strengthened its commitment to conducting human rights impact assessments (G4). The company also improved its engagement with stakeholders by joining the GNI (G5). Notably, Telefónica improved its disclosure on grievance and remedy mechanisms, and received the highest score of all 22 companies in the Index on this indicator (G6),[4] although the company did not provide clear evidence that it is responding to these complaints.

Freedom of Expression 33%

Telefónica ranked third among the 10 telecommunications companies in the Freedom of Expression category, behind Vodafone and AT&T.

Content and account restriction requests: Telefónica disclosed little about how it handles government or private requests to block content or accounts (F5-F7), but it was among only three telecommunications companies in the Index to publish transparency reports. It provided more data on the number of government requests it received and complied with, including the number of URLs affected (F6).[5] Like its peers, Telefónica published nothing about private requests to block content or accounts (F7).

Network management and shutdowns: As in the 2017 Index, Telefónica Spain disclosed almost no information about its network management policies, receiving the second-lowest score of all telecommunications companies on this indicator (F9). Yet, along with Vodafone UK, it was more transparent than the rest of its peers about how it handles government demands to shut down networks (F10). The company improved its disclosure of why it may reject a network shutdown demand and provided more detailed data about its compliance with these types of requests.

Identity policy: Telefónica Spain disclosed that it requires pre-paid mobile users to provide government-issued identification, which is legally required in Spain (F11).[6]

Privacy 32%

Telefónica ranked third out of the 10 telecommunications companies in the Privacy category, behind AT&T and Vodafone.

Handling user information: Telefónica Spain disclosed less than AT&T and Vodafone UK but slightly more than Orange France and América Móvil's Telcel about how it handles user information (P3-P8). It had the highest score of all telecommunications companies on what user information it collects (P3), and for what purpose (P5), but disclosed nothing about what user information it shares (P4), for how long it retains it (P6), or whether users can obtain all of the information the company holds on them (P8). It disclosed some options for users to control what information it collects, including for the purposes of targeted advertising, but did not reveal if targeted advertising is off by default (P7).

Requests for user information: Telefónica disclosed less than AT&T and Vodafone about how it handles government and private requests for user information (P10-P11). It improved its disclosure of its process for responding to government requests for user information by clarifying why it may reject a government request (P10). The company also provided more data on government and private requests for user information, including the number of accounts affected (P11).[7] Like the rest of its peers, Telefónica did not disclose a policy of notifying users if their information is requested (P12).

Security: Telefónica Spain disclosed less than AT&T and Vodafone UK about is security policies and practices, but more than the rest of its peers (P13-P18). Although it disclosed it limits employee access to user information, it did not disclose it has systems in place to monitor this (P13). Like most telecommunications companies, the company did not disclose a bug bounty program allowing security researchers to submit vulnerabilities (P14). It received the second-highest score in the Index, after Vodafone UK, for disclosure of its processes for responding to data breaches (P15).

[5] "Report on Transparency in Communications," Telefónica, 2017, https://www.telefonica.com/documents/153952/183394/Informe_Transparencia_Comunicaciones_Telefonica_EN.pdf/30519143-d3ab-50c3-1cb5-319a735fd9d3.
[6] "Ley 25/2007, de 18 de Octubre, de Conservación de Datos Relativos a Las Comunicaciones Electrónicas Y a Las Redes Públicas de Comunicaciones," (2007).
[7] "Report on Transparency in Communications," Telefónica, 2017.

Telecommunications Company

Vodafone Group Plc.

OPERATING COMPANY EVALUATED
- **Vodafone UK**

SERVICES EVALUATED
- **Pre-paid mobile**
- **Post-paid mobile**
- **Fixed-line broadband**

RANK: 1

SCORE: 52%

DIFFERENCE FROM 2017: ^ 3.47

RANK AMONG 10 TELECOMMUNICATIONS COMPANIES

Key Findings:

- Vodafone earned the top score among telecommunications companies, and disclosed more about policies and practices affecting freedom of expression than the rest of its peers.
- Vodafone was the only company out of all 22 companies evaluated in the Index to provide comprehensive information on the company's response to data breaches.
- The company disclosed little regarding how users can control the company's handling of their user information, and failed to make a commitment to turn off targeted advertising by default.

Key Recommendations:

- **Be transparent about government requests.** Vodafone should better inform users about different third party requests it receives, including government requests to shut down a network, and disclose where laws may prevent the company from being fully transparent.
- **Clarify its handling of user data.** The company should be more clear about what user information it collects and shares, and for how long it retains this information.
- **Make user privacy the default setting.** The company should give users more options to control their own data and clearly commit to turn off targeted advertising by default.

Analysis

Vodafone was the highest scoring company out of all 10 telecommunications companies evaluated.[1] In addition to other improvements, the company strengthened its commitment to protecting users' human rights by joining the Global Network Initiative (GNI) in March 2017. At the corporate level, Vodafone made strong commitments to protect freedom of expression and privacy as human rights, but there is room for improvement. The company should provide clear evidence that it responds to complaints from users who believe their rights to freedom of expression and privacy were violated by the company (G6). The company should also provide users with more options to control collection of their user information, and it should commit to turn off targeted advertising by default (P7). Notably, Vodafone was the only company out of all 22 companies evaluated in the Index to clearly disclose its process for handling data breaches (P15).

Vodafone Group Plc.

Vodafone Group Plc provides telecommunications services in Europe, Asia, Middle East, and Africa. The company serves 516 million mobile, 17.9 million fixed broadband, and 13.8 million TV customers.[2]

Market Cap: USD 77.3 billion[3]
LSE: VOD
Domicile: United Kingdom
Website: www.vodafone.com

[1] The research period for the 2018 Index ran from January 13, 2017 to January 12, 2018. Policies that came into effect after January 12, 2018 were not evaluated in this Index. For Vodafone's performance in the 2017 Index, see: https://rankingdigitalrights.org/index2017/companies/vodafone.
[2] 2017 Vodafone Annual Report, http://www.vodafone.com/content/annualreport/annual_report17/downloads/Vodafone-full-annual-report-2017.pdf.
[3] Bloomberg Markets, Accessed February 26, 2018, https://www.bloomberg.com/quote/VOD:LN.

Governance 84%

Vodafone was the highest-scoring telecommunications company in the Governance category. Vodafone publicly committed to respect freedom of expression and privacy as human rights (G1), and provided evidence of senior level oversight over these issues within the company (G2). Vodafone improved its disclosure of human rights impact assessments, but there continues to be room for improvement (G4). Company disclosure also improved in terms of stakeholder engagement due to Vodafone joining the GNI in March 2017 (G5). Vodafone tied with Bharti Airtel for the second highest score on disclosure of its grievance and remedy mechanisms (G6); however, gaps in disclosure remained. While Vodafone provided users with several options to submit complaints, including those related to freedom of expression and privacy, it offered no information about the number of complaints it received or any evidence that it is responding to them.

Freedom of Expression 46%

Vodafone was the highest-scoring telecommunications company in the Freedom of Expression category, outscoring AT&T by five percentage points and Telefónica by more than ten points.

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

Network management and shutdowns: Vodafone UK earned the highest score for its disclosure of network management policies, and it was the only company to receive full credit for clearly committing not to block or prioritize content (F9). Despite making improvements to its disclosure of network shutdowns, it did not disclose how many shutdown requests it received or with which it complied (F10). Under limited circumstances, UK law may prevent telecommunications operators from disclosing certain government requests to shut down a network. The company should clearly inform users about these restrictions.[4]

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

Privacy 44%

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

Handling of user information: Vodafone UK disclosed more than most of its peers about how it handles user information, but less than AT&T (P3-P8). However, it still did not sufficiently disclose what user information it collects (P3), shares (P4), and why (P5). It disclosed little about how long it retains user information (P6), but it was the only telecommunications company besides AT&T to disclose anything about these policies. Vodafone UK did not disclose whether users can control collection of their own information or whether users can delete some of this information. It clearly explained how users can opt out of having their information used for advertising purposes, but it failed to disclose that targeted advertising is off by default (P7).

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

Security: Vodafone UK disclosed more than any other telecommunications company about its security policies (P13-P18). Notably, it was the only company out of all 22 companies evaluated in the Index to provide comprehensive information on its handling of data breaches (P15). However, the company did not disclose anything about how it addresses security vulnerabilities (P14).

[4] For more information, see sections 252, 253, and 255(8) of the Investigatory Powers Act (2016): http://www.legislation.gov.uk/ukpga/2016/25/section/253/enacted.

11. Appendix

11.1 Index methodology development

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

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

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

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

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

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

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 at: https://www.rankingdigitalrights.org/index2018/download/.

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
- F7, 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

- 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

Endnotes

1. Figures as of March 8, 2018. Bloomberg Markets, https://www.bloomberg.com/markets.

2. Figures as of December 31, 2017. "World Internet Users Statistics and 2018 World Population Stats," Internet World Stats, accessed March 19, 2018, https://www.internetworldstats.com/stats.htm.

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

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

5. "Principles," Global Network Initiative, accessed February 27, 2017, https://globalnetworkinitiative.org/principles/index.php.

6. "Implementation Guidelines," Global Network Initiative, accessed February 28, 2017, http://globalnetworkinitiative.org/implementationguidelines/index.php.

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

8. "2018 Companies," Ranking Digital Rights, https://rankingdigitalrights.org/2018-companies/.

9.For the full set of indicators, definitions, and research guidance please visit: "2018 Indicators," Ranking Digital Rights, https://rankingdigitalrights.org/2018-indicators/.

10. "2018 Indicators: Governance," Ranking Digital Rights, https://rankingdigitalrights.org/2018-indicators/#G.

11. "2018 Indicators: Freedom of Expression," Ranking Digital Rights, https://rankingdigitalrights.org/2018-indicators/#F.

12. "2018 Indicators: Privacy," Ranking Digital Rights, https://rankingdigitalrights.org/2018-indicators/#P.

13. Julia Carrie Wong, "Mark Zuckerberg Apologises for Facebook's 'mistakes' over Cambridge Analytica," *The Guardian*, March 22, 2018, https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica.

14. Zack Whittaker, "Orbitz Says Hacker Stole Two Years' Worth of Customer Data," *ZDNet*, March 20, 2018, http://www.zdnet.com/article/orbitz-says-hacker-stole-customer-data/.

15. Yarno Ritzen, "Rising Internet Shutdowns Aimed at 'Silencing Dissent,'" *Al Jazeera*, January 29, 2018, https://www.aljazeera.com/news/2018/01/rising-internet-shutdowns-aimed-silencing-dissent-180128202743672.html.

16. "2018 Edelman Trust Barometer," Edelman, accessed March 23, 2018, https://www.edelman.com/trust-barometer.

17. "Executive Summary - 2017 Internet Society Global Internet Report: Paths to Our Digital Future," Internet Society, 2017, https://future.internetsociety.org/introduction/executive-summary/.

18. “Chinese Internet Companies Show Room for Improvement,” Ranking Digital Rights, March 23, 2017, https://rankingdigitalrights.org/index2017/findings/china/.

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

20. “GNI Principles on Freedom of Expression and Privacy” Global Network Initiative, accessed February 27, 2017, https://globalnetworkinitiative.org/principles/index.php.

21. “Implementation Guidelines for the Principles on Freedom of Expression and Privacy” Global Network Initiative, accessed March 26, 2018, http://globalnetworkinitiative.org/implementationguidelines/index.php.

22. “Telecommunications Industry Dialogue Launches Final Annual Report,” Telecommunications Industry Dialogue, September 21, 2017, http://www.telecomindustrydialogue.org/telecommunications-industry-dialogue-launches-final-annual-report/.

23. Malachy Browne, “YouTube Removes Videos Showing Atrocities in Syria,” *The New York Times*, August 22, 2017, https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html.

24. Thant Sin, “Facebook Bans Racist Word ‘Kalar’ in Myanmar, Triggers Collateral Censorship,” Global Voices, June 2, 2017, https://advox.globalvoices.org/2017/06/02/facebook-bans-racist-word-kalar-in-myanmar-triggers-collateral-censorship/.

25. “Microsoft Salient Human Rights Issues: Report - FY17,” Microsoft, http://download.microsoft.com/download/6/9/2/692766EB-D542-49A2-AF27-CC8F9E6D3D54/Microsoft_Salient_Human_Rights_Issues_Report-FY17.pdf.

26. For more information, see sections 252, 253, and 255(8) of the Investigatory Powers Act: http://www.legislation.gov.uk/ukpga/2016/25/section/253/enacted.

27. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation),” (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

28. David Kaye, “How Europe’s New Internet Laws Threaten Freedom of Expression,” *Foreign Affairs*, December 18, 2017, https://www.foreignaffairs.com/articles/europe/2017-12-18/how-europes-new-internet-laws-threaten-freedom-expression.

29. “Code of Conduct on Countering Illegal Hate Speech Online First Results on Implementation” (European Commission, December 2016) https://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf.

30. “Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)” (2017), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf and Ben Knight, “Germany Implements New Internet Hate Speech Crackdown,” *DW*, January 1, 2018, http://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590.

31. “EU: European Commission’s Code of Conduct for Countering Illegal Hate Speech Online and the Framework Decision - Legal Analysis” (Article 19, June 2016), https://www.article19.org/data/files/medialibrary/38430/EU-Code-of-conduct-analysis-FINAL.pdf.

32. Emma Lux, "Efforts to Curb Fraudulent News Have Repercussions around the Globe," Reporters Committee for Freedom of the Press, December 6, 2017, https://www.rcfp.org/browse-media-law-resources/news/efforts-curb-fraudulent-news-have-repercussions-around-globe.

33. "Factsheet on the Code of Conduct – 3 round of monitoring" (European Commission, January 2018) document available here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086.

34. See for example Olivia Solon, "'I Can't Trust YouTube Any More': Creators Speak out in Google Advertising Row," *The Guardian*, March 21, 2017, https://www.theguardian.com/technology/2017/mar/21/youtube-google-advertising-policies-controversial-content and Thant Sin, "Facebook Bans Racist Word 'Kalar' in Myanmar, Triggers Collateral Censorship," Global Voices, June 2, 2017, https://globalvoices.org/2017/06/02/facebook-bans-racist-word-kalar-in-myanmar-triggers-collateral-censorship/.

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

36. 2017 Corporate Accountability Index, Ranking Digital Rights, https://rankingdigitalrights.org/index2017/assets/static/download/RDRindex2017report.pdf.

37. 2018 Index Indicators, https://rankingdigitalrights.org/index2018/indicators/p15.

38. "Guidelines for Protection of Critical Information Infrastructure" (National Critical Information Infrastructure Protection Centre, January 16, 2015), http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.

39. "2017: Poor Internal Security Practices Take a Toll," Breach Level Index (Gemalto, 2017), http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf.

40. Christina Wood, "Insider Threat Examples: 7 Insiders Who Breached Security," *CSO Online*, March 19, 2018, https://www.csoonline.com/article/3263799/security/insider-threat-examples-7-insiders-who-breached-security.html.

41. See 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P13.

42. AT&T Privacy Policy, "What safeguards does AT&T have in place?" accessed March 20, 2018, http://about.att.com/sites/privacy_policy/full_privacy_policy.

43. See the 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P14.

44. Nathalie Maréchal, "Global Inequality in Your Pocket: How Cheap Smartphones and Lax Policies Leave Us Vulnerable to Hacking," *Global Voices Advocacy*, March 30, 2017, https://advox.globalvoices.org/2017/03/30/global-inequality-in-your-pocket-how-cheap-smartphones-and-lax-policies-leave-us-vulnerable-to-hacking/.

45. Nicole Perlroth, "iPhone Users Urged to Update Software After Security Flaws are Found," *The New York Times*, August 25, 2016, https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html.

46 . "Hungarian Hacker Arrested for Pressing F12," *TechCrunch*, July 25, 2017, https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/.

47. Zack Whittaker, "Lawsuits Threaten Infosec Research - Just When We Need It Most." *ZDNet*, February 19, 2018, www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/.

48. Dipayan Ghosh 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/.

49. "Sorry Just Isn't Enough. Businesses Must Do Better When It Comes To People's Data," Internet Society, March 23, 2018, https://www.internetsociety.org/news/statements/2018/sorry-just-isnt-enough-businesses-must-better-comes-peoples-data/.

50. See the 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/.

51. See Chapter 6, 2017 Corporate Accountability Index, Ranking Digital Rights, https://rankingdigitalrights.org/index2017/assets/static/download/RDRindex2017report.pdf.

52. See the "Advertising identifiers on mobile devices" section of Google's Advertising page for more information: "Advertising," Google Privacy & Terms, accessed March 23, 2018, https://www.google.com/policies/technologies/ads/.

53. Recent examples illustrate how advertising tools on social media have been exploited to spread disinformation during the 2016 U.S. presidential elections and the Brexit referendum:

> "Russian Twitter Trolls Meddled in the Brexit Vote. Did They Swing It?," *The Economist*, November 23, 2017, https://www.economist.com/news/britain/21731669-evidence-so-far-suggests-only-small- campaign-new- findings-are-emerging-all;
>
> Alex Hern, "Facebook Enables 'fake News' by Reliance on Digital Advertising – Report," *The Guardian*, January 31, 2018, https://www.theguardian.com/technology/2018/jan/31/facebook-fake-news-disinformation-digital-advertising-report-news-feed.
>
> Researchers have similarly shown how these tools can be used by white supremacists to spread hateful messages against Jewish and Muslim communities: Will Oremus and Bill Carey, "Facebook's Offensive Ad Targeting Options Go Far Beyond 'Jew Haters,'" *Slate Future Tense*, September 14, 2017, http://www.slate.com/blogs/future_tense/2017/09/14/facebook_let_advertisers_target_jew_haters_it_doesn_t_end_there.html.

54. 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/.

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

56. See more information on this Facebook help page: "How Does Facebook Decide Which Ads to Show Me and How Can I Control the Ads I See?," Facebook Help Center, accessed March 20, 2018, https://www.facebook.com/help/562973647153813?helpref=faq_content.

57. See the 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P9.

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

59. See Twitter's disclosure: "Do Not Track," Twitter Help Center, accessed March 26, 2018, https://help.twitter.com/en/safety-and-security/twitter-do-not-track.

60. "Universal Declaration of Human Rights" (United Nations, December 10, 1948), http://www.un.org/en/universal-declaration-human-rights/ and "International Covenant on Civil and Political Rights" (United Nations, December 16, 1966), http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

61. "2018 Indicators: Freedom of Expression," see F3-F10: https://rankingdigitalrights.org/2018-indicators/#F.

62. See Chapter 5, 2017 Corporate Accountability Index, Ranking Digital Rights, https://rankingdigitalrights.org/index2017/assets/static/download/RDRindex2017report.pdf.

63. "Hard Questions: How We Counter Terrorism," Facebook Newsroom, June 15, 2017, https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/.

64. YouTube, "How Content ID Works," accessed March 19, 2018, https://support.google.com/youtube/answer/2797370.

65. 2015 Corporate Accountability Index, Ranking Digital Rights, p. 25, https://rankingdigitalrights.org/index2015/assets/static/download/RDRindex2015report.pdf.

66. See p. 29-30, 2017 Corporate Accountability Index, Ranking Digital Rights, https://rankingdigitalrights.org/index2017/assets/static/download/RDRindex2017report.pdf.

67. "An update on our efforts to combat violent extremism," Twitter Blog, August 18, 2016, https://blog.twitter.com/official/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.html.

68. Twitter Government TOS Report, https://transparency.twitter.com/en/gov-tos-reports.html.

69. Microsoft Content Removal Requests report, https://www.microsoft.com/en-us/about/corporate-responsibility/crrr/.

70. "Why flagging matters," YouTube Official Blog, September 15, 2016, https://youtube.googleblog.com/2016/09/why-flagging-matters.html.

71. "Improvements in protecting the integrity of activity on Facebook," Facebook Security, April 12, 2017. https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766.

72. Richard Allan, "Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community?" Facebook Newsroom, June 27, 2018, https://newsroom.fb.com/news/2017/06/hard-questions-hate-speech/.

73. "Growing Our Trusted Flagger Program into YouTube Heroes," Official YouTube Blog, September 22, 2016, https://youtube.googleblog.com/2016/09/growing-our-trusted-flagger-program.html.

74. "Growing our Trusted Flagger program into YouTube Heroes," YouTube Official Blog, September 22, 2016, https://youtube.googleblog.com/2016/09/growing-our-trusted-flagger-program.html.

75. Press Association, "YouTube Introduces New Measures to Curb Extremist Video Online," *The Guardian*, June 19, 2017, https://www.theguardian.com/technology/2017/jun/18/more-must-be-done-about-extremist-content-online-says-google.

76. "Press Release - European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech," European Commission, May 31, 2016, http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

77. Ismira Lutfia Tisnadibrata, "Indonesia: Google, Twitter Agree to Tighten Content Monitoring," *BenarNews*, August 4, 2017, https://www.benarnews.org/english/news/indonesian/indonesia-terrorism-08042017183754.html.

78. "What We Do," Internet Watch Foundation, accessed March 22, 2018, https://www.iwf.org.uk/what-we-do.

79. "Fact sheet on the Right to be Forgotten Ruling," European Commission, https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf.

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

81. Farhad Manjoo, "Clearing Out the App Stores: Government Censorship Made Easier," *The New York Times*, January 18, 2018, https://www.nytimes.com/2017/01/18/technology/clearing-out-the-app-stores-government-censorship-made-easier.html.

82. Paul Mozur, "Skype Vanishes From App Stores in China, Including Apple's," *The New York Times*, November 21, 2017, https://www.nytimes.com/2017/11/21/business/skype-app-china.html.

83. Tim Bradshaw, "Apple drops hundreds of VPN apps at Beijing's request," *Financial Times*, November 21, 2017, https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc.

84. See "Global Network Initiative Adds Seven Companies in Milestone Expansion of Freedom of Expression and Privacy Initiative | Global Network Initiative," Global Network Initiative, March 27, 2017, https://www.globalnetworkinitiative.org/news/global-network-initiative-adds-seven-companies-milestone-expansion-freedom-expression-and and "Telecommunications Industry Dialogue Launches Final Annual Report," Telecommunications Industry Dialogue, September 21, 2017, http://www.telecomindustrydialogue.org/telecommunications-industry-dialogue-launches-final-annual-report/.

85. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

86. "A/HRC/35/22: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (United Nations Human Rights Council, March 30, 2017), https://ccdcoe.org/sites/default/files/documents/UN-170726-AHRC3522.pdf.

87. "A/HRC/35/22: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (United Nations Human Rights Council, March 30, 2017), https://ccdcoe.org/sites/default/files/documents/UN-170726-AHRC3522.pdf.

88. "Law Enforcement Disclosure Statement: Digital Rights and Freedoms," Vodafone, May 2017, http://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_statement.pdf.

89. "Resolution A/HRC/32/L.20 on the Promotion, Protection and Enjoyment of Human Rights on the Internet" (United Nations Human Rights Council, June 30, 2016), https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

90. "Launching STOP: the #KeepItOn internet shutdown tracker," Access Now, November 16, 2017, https://www.accessnow.org/keepiton-shutdown-tracker/.

91. "Internet Shutdowns," Software Freedom Law Center, accessed March 21, 2018, https://www.internetshutdowns.in/.

92. "Global Network Initiative and Telecommunications Industry Dialogue Joint Statement on Network and Service Shutdowns," Global Network Initiative, July 12, 2016, https://globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-joint-statement-network-and.

93. "The Freedom Online Coalition Joint Statement on State Sponsored Network Disruptions" (Freedom Online Coalition, 2017), https://www.freedomonlinecoalition.com/wp-content/uploads/2017/03/FOCJointStatementonStateSponsoredNetworkDisruptions.docx.pdf.

94. See "Network Shutdowns" in the 2017 Index: "Network Shutdowns: Users Are in the Dark about Why They're Cut Off," https://rankingdigitalrights.org/index2017/findings/networkshutdowns/.

95. "License Agreement for Provision of Internet Services" (Government of India Ministry of Communications & IT), accessed March 14, 2018, http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf, "License Agreement for Provision of United Access Services after Migration from CMTS" (Government of India Ministry of Communications & IT, December 3, 2009), http://www.auspi.in/policies/UASL.pdf, and "License Agreement for Unified License" (Government of India Ministry of Communications & IT), accessed March 14, 2018, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.

96. "Public Telecommunications License No. 1/2006" Telecommunications Regulatory Authority, accessed March 15, 2018, https://www.tra.gov.ae/assets/03VgXUV3.pdf.aspx and "CLFR - Qatar," Global Network Initiative, January 8, 2018, https://globalnetworkinitiative.org/content/clfr-qatar.

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

98. See the 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/.

99. Michalsons, "Protection of Personal Information Act Summary," Michalsons, accessed March 20, 2018, https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia.

100. “International Principles on the Application of Human Rights to Communications Surveillance,” Necessary and Proportionate, accessed March 22, 2018, https://necessaryandproportionate.org/.

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

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

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

104. “International Principles on the Application of Human Rights to Communications Surveillance,” Necessary and Proportionate, accessed March 22, 2018, https://necessaryandproportionate.org/principles.

105. “Manila Principles on Intermediary Liability,” Manila Principles, accessed March 22, 2018, https://www.manilaprinciples.org/.

106. Global Commission on Internet Governance, “One Internet,” Centre for International Governance Innovation, June 21, 2016, https://www.cigionline.org/publications/one-internet.

107. Ben Eisen, “Facebook Stock Decline Knocks It Out of S&P 500's Big Five,” *Wall Street Journal*, March 19, 2018, https://blogs.wsj.com/moneybeat/2018/03/19/facebook-stock-decline-knocks-it-out-of-sp-500s-big-five/.

108. “2018 Companies,” Ranking Digital Rights, https://rankingdigitalrights.org/2018-companies/.

109. Figures as of December 31, 2017. “World Internet Users Statistics and 2018 World Population Stats,” Internet World Stats, accessed March 19, 2018, https://www.internetworldstats.com/stats.htm.