



**RANKING DIGITAL RIGHTS**

# 2015 Corporate Accountability Index

*The Ranking Digital Rights 2015 Corporate Accountability Index evaluates 16 of the world's most powerful Internet and telecommunications companies on their commitments, policies, and practices that affect users' freedom of expression and privacy.*

NOVEMBER 2015

*Developed in partnership with*



## Acknowledgements

### Ranking Digital Rights staff:

**Rebecca MacKinnon**, Director

**Allon Bar**, Research Coordinator and  
Human Rights Specialist

**Priya Kumar**, Research Analyst

**Tim Libert**, Open Technology Fund Fellow

For a full list of all people who contributed research for this Index please see [rankingdigitalrights.org/who/affiliates](https://rankingdigitalrights.org/who/affiliates).

The 2015 Corporate Accountability Index, plus related methodological research and stakeholder consultations conducted by the Ranking Digital Rights project since 2013, was supported by the following funders:

- John D. and Catherine T. MacArthur Foundation
- John S. and James L. Knight Foundation (2014 Knight News Challenge)
- Ford Foundation
- Open Society Foundations
- The William and Flora Hewlett Foundation
- The Shuttleworth Foundation (Flash Grant)
- Media Democracy Fund
- Hivos People Unlimited
- Global Engagement Fund (Provost's Office, 2013), University of Pennsylvania
- Internews Center for Innovation and Learning

For a full list of institutional partners please see the project website at [rankingdigitalrights.org/who/partners](https://rankingdigitalrights.org/who/partners).

## About Ranking Digital Rights

Ranking Digital Rights is a non-profit research initiative housed at New America's Open Technology Institute in Washington D.C., working with an international network of partners to promote greater respect for freedom of expression and privacy by focusing on the policies and practices of companies in the information communications technology (ICT) sector. For more information, please visit [rankingdigitalrights.org](https://rankingdigitalrights.org).

## About Sustainalytics

Headquartered in Amsterdam, Sustainalytics is an independent ESG and corporate governance research, ratings, and analysis firm supporting investors around the world with the development and implementation of responsible investment strategies. With 13 offices globally, Sustainalytics partners with institutional investors who integrate environmental, social and governance information and assessments into their investment processes. Today, the firm has 230 staff members, including more than 120 analysts with varied multidisciplinary expertise across more than 40 sectors. For the past three years, Sustainalytics has been named the best independent responsible investment research firm in Extel's IRRI survey of institutional investors. For more information, visit [sustainalytics.com](https://sustainalytics.com).

## **Contents**

Executive summary	4
<b>1. INTRODUCTION</b>	<b>6</b>
1.1 What and why	6
1.2 Our approach	9
<b>2. KEY FINDINGS</b>	<b>11</b>
2.1 The bad news	12
2.2 The good news	14
<b>3. RECOMMENDATIONS</b>	<b>16</b>
3.1 For companies	16
3.2 For governments	18
3.3 For all others: Individuals, advocates, activists, investors, and researchers	18
<b>4. CATEGORY ANALYSIS</b>	<b>20</b>
4.1 Commitment	20
4.2 Freedom of expression	22
4.3 Privacy	27

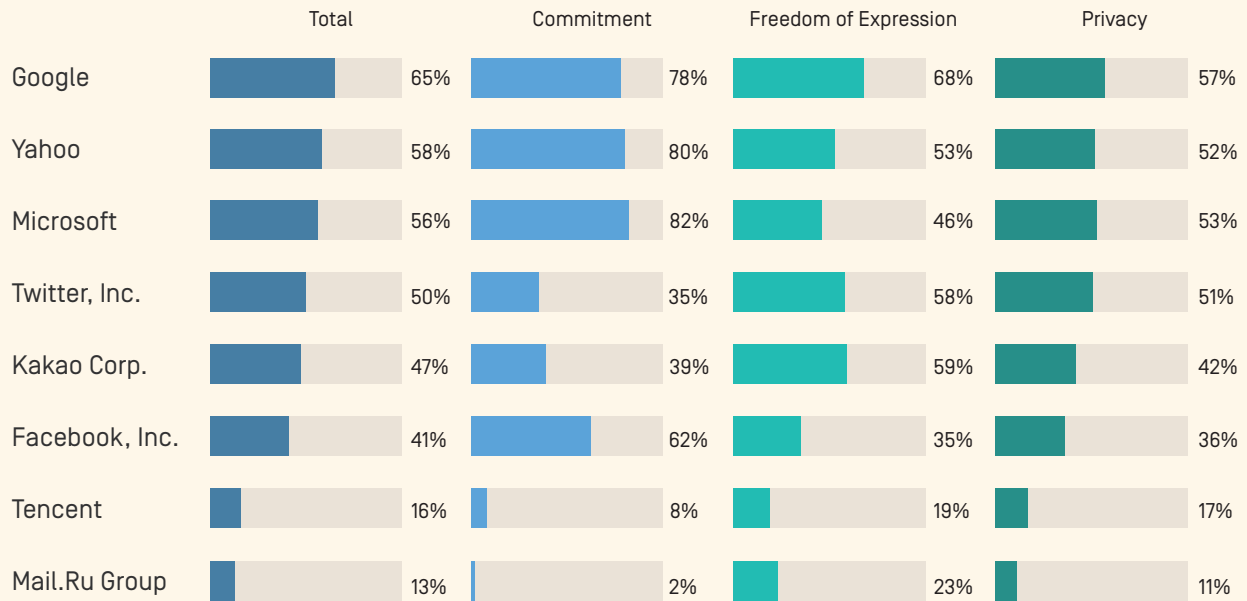
<b>5. COMPANY REPORTS</b>	32
<b>5.1 Internet Companies</b>	33
Facebook, Inc	33
Google	35
Kakao Corp.	37
Mail.ru Group	39
Microsoft	41
Tencent	43
Twitter, Inc	45
Yahoo	47
<b>5.2 Telecommunications Companies</b>	49
América Móvil	49
AT&T	51
Axiata	54
Bharti Airtel	56
Etisalat	59
MTN	61
Orange	64
Vodafone	67
<b>6. APPENDIX</b>	70
6.1. Methodology	70
6.2. Table of Company Results Per Indicator	76

# CORPORATE ACCOUNTABILITY INDEX

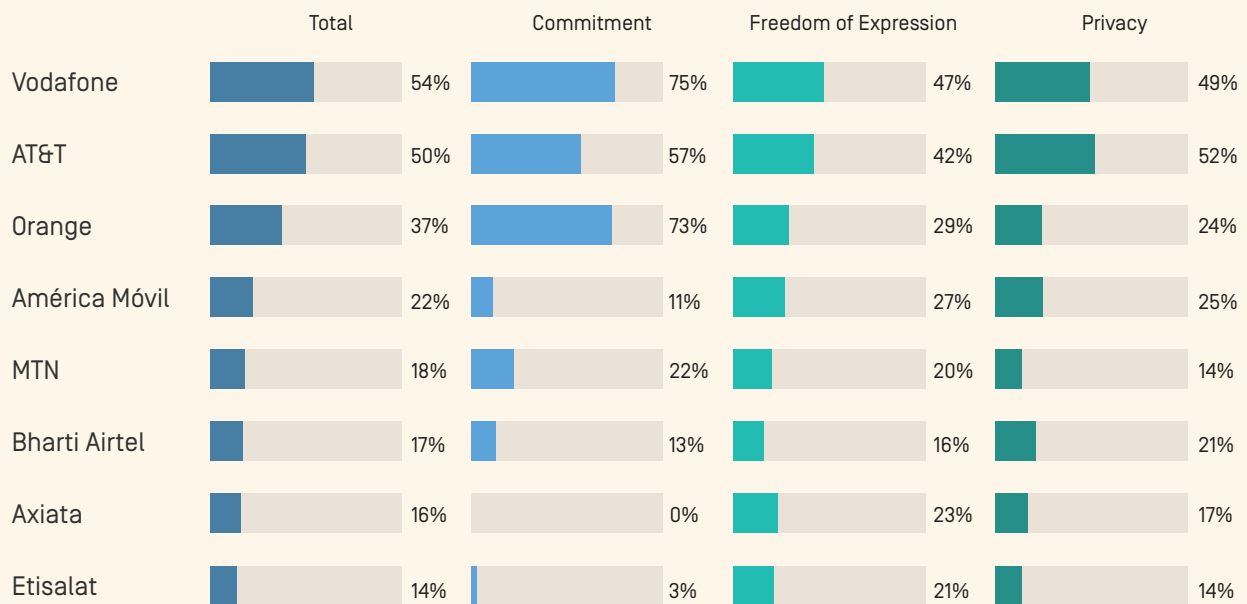
## Overall results for Internet and telecommunications companies

Results are tallied from 31 indicators across three categories: Commitment, Freedom of Expression, and Privacy.

### INTERNET COMPANIES



### TELECOMMUNICATIONS COMPANIES



# EXECUTIVE SUMMARY

---

Ranking Digital Rights' inaugural **Corporate Accountability Index** evaluates 16 of the world's most powerful Internet and telecommunications companies on their commitments, policies, and practices that affect users' freedom of expression and privacy.

By opening the door for greater corporate transparency and public scrutiny of business practices, the Index encourages companies to do a better job of respecting their users' rights around the globe.

To view in-depth results, download data, and access related resources, news, and updates, please visit: [rankingdigitalrights.org](https://rankingdigitalrights.org)

## Highlights

**There are no "winners." Even companies in the lead are falling short.**

Across the board, companies need to improve their disclosure of policies and practices that affect users' freedom of expression and privacy, as well as their commitments to these human rights.

- Only six companies scored at least 50 percent of the total possible points. The highest score was only 65 percent.
- Nine companies scored at least 30 percent, the minimum threshold for companies to demonstrate meaningful effort to respect users' rights.
- Seven companies – nearly half – scored between 13-22 percent, demonstrating a serious deficit of respect for users' freedom of expression and privacy.

**Users are left in the dark about many company practices that affect freedom of expression and privacy.**

No company in the Index provides users with sufficiently clear, comprehensive, and accessible information about their practices that affect freedom of expression and privacy. These practices include companies' handling of user information, terms of service enforcement, and government and private requests to restrict content or

share user information. Without such information it is difficult to hold companies, governments, and other actors accountable when users' rights are undermined.

- **Disclosure about collection, use, sharing, and retention of user information is poor.** Even companies that make efforts to publish such information still fail to communicate clearly with users about what is collected about them, with whom it is shared, under what circumstances, and how long the information is kept.
- **Disclosure about private and self-regulatory processes is minimal and ambiguous at best, and often non-existent.** Few companies disclose data about private third-party requests to remove or restrict content or to share user information – even when those requests come with a court order or subpoena, or are made in accordance with established legal processes such as a copyright “notice-and-takedown” system. Even fewer companies disclose any information about whether – let alone how – they receive or respond to private or informal requests. Further, no companies in the Index disclose any information about actions they have taken to enforce their terms of service.
- **In some instances, current laws and regulations make it more difficult for companies to respect freedom of expression and privacy.** However, there are still actions companies can take to improve. All of the ranked companies face some legal or regulatory requirements that hinder their performance on certain indicators. For example, laws in many countries forbid companies from disclosing national-security related government requests. Some companies face more domestic political, legal, and regulatory obstacles to respecting users' rights than others, because some countries' political and legal frameworks are less compatible with international human rights standards. Nonetheless, we have identified ways that all companies can improve their performance, even without changes to their political, legal, and regulatory environments.

## There is also good news:

- **Each of the companies in the Index is doing something well.** All of the companies we evaluated have at least some practices and/or policies in place that help to protect freedom of expression or privacy.
- **“Transparency reporting” is becoming a standard practice.** Nine of the 16 ranked companies publish some information about requests they receive from governments or private parties to share user information, and/or to remove or block content, deactivate accounts, or deny access to service.
- **Seven of the companies (nearly half) have backed up their commitments to freedom of expression and privacy by disclosing the concrete measures they have taken to implement those commitments.** Such measures include employee training and whistleblowing mechanisms, internal oversight and accountability processes, and human rights impact assessments.

## Key recommendations for companies:

Based on our findings, we have developed a set of practical and immediate steps that companies can take to better respect their users’ freedom of expression and privacy, thereby boosting user trust and winning the confidence of responsible investors.

- **Disclose and communicate information that all stakeholders can understand, not just telecommunications regulators or Internet policy specialists.** Some companies state that they are compliant with the law but provide little or no explanation of how that compliance affects users. Companies need to disclose information in an accessible and user-friendly manner so that people understand the potential risks they may face.
- **Communicate clearly with users about what happens to their information.** If somebody were to create a dossier or “file” on the user based on the information the company holds about them, what would it look like? For users to know the answer to that question, companies need to disclose sufficient information about what data they collect, how they use it, how long they keep it, with whom they share it, and under what circumstances they share it.

- **Demonstrate a credible commitment to security.** Companies should provide evidence that they maintain industry standards of encryption and security, educate users about potential threats, and disclose basic information about their security practices, including whether employee access to user information is monitored and whether the company conducts security audits.
- **Carry out due diligence to understand and address the impact of products, services, and business operations on users’ rights.** Companies that are serious about respecting users’ human rights need to undertake regular impact assessments that examine potential risks to freedom of expression and privacy. In order to be credible, the quality and scope of these assessments should be verified by an independent multi-stakeholder organization committed to human rights principles.
- **Provide concrete evidence that the company has institutionalized its commitments.** While it is important for company leaders to demonstrate strong personal commitments to users’ rights, it is even more important that such commitments be clearly institutionalized. Otherwise, users, investors, and other stakeholders have no way of knowing whether practices will change or stay the same after key people leave the company.
- **Establish effective grievance and remedy mechanisms.** Companies should develop channels for users and other affected parties to file grievances if they feel that their freedom of expression and/or privacy have been violated in connection with use of the company’s service. Companies must also develop concrete processes for responding to and remedying these complaints.

**We must all advocate for legal and regulatory changes that enable companies to respect users’ freedom of expression and privacy.** Everyone – companies, civil society activists, citizens, responsible investors, and policy-makers – must all advocate for change. Full corporate accountability will only be achieved when governments are also held accountable. We must work together to build legal, regulatory, and corporate standards that make it possible to protect and respect human rights.

Comparative data of company results, including data for each individual company and indicator, can be viewed and downloaded from the project website at [rankingdigitalrights.org](http://rankingdigitalrights.org).

# INTRODUCTION

---

The 2015 Ranking Digital Rights Corporate Accountability Index evaluates 16 of the world's most powerful Internet and telecommunications companies on their commitments and policies that affect users' freedom of expression and privacy.

The companies ranked in this Index collectively affect the lives of billions of people across the world. People increasingly depend on Internet and telecommunications services for many facets of their daily lives, including civic, political, and religious activities. The services these companies offer connect and empower people in unprecedented ways, but they can also be misused to undermine freedom of expression and privacy.

Companies are losing public trust. According to a recent Gallup poll, only about two in 10 Americans said they "have a lot of trust in the companies they regularly do business with to keep their personal information secure."<sup>1</sup> In a 2014 poll of Internet users in 24 countries commissioned by the Center for International Governance Innovation, 74 percent of respondents said they are "concerned about company monitoring of online activity and the subsequent sale of personal data."<sup>2</sup> Loss of trust represents a material risk for companies' business.

At the same time, society places a complex set of expectations and responsibilities upon these companies: we want them to be innovative, to make life easier and more enjoyable, and to help make our economic and business activities more efficient. We want them to operate in a way that supports public safety, child protection, and national security. In doing so, however, companies face demands from governments and others to facilitate censorship and surveillance.

Like all other businesses, the companies in this Index, and the broader technology sector they represent, share a **responsibility to respect human rights**.<sup>3</sup>

---

1. John Fleming and Daniela Yu, "Consumers Doubt Their Personal Info is Safe," Gallup Business Journal, March 11, 2015, <http://www.gallup.com/businessjournal/181904/consumers-doubt-personal-info-safe.aspx>.

2. Centre for International Governance Innovation & IPSOS, CIGI-Ipsos Global Survey on Internet Security and Trust, <https://www.cigionline.org/internet-survey>.

3. United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, HR/PUB/11/04 (2011), [http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

Freedom of expression and privacy are rights guaranteed in key international human rights frameworks, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The international community has affirmed that these rights should extend to the digital realm.<sup>4</sup> By evaluating and comparing companies' commitments, policies, and disclosures about practices that impact users' freedom of expression and privacy, the Corporate Accountability Index seeks to:

- Help companies understand what changes they should make to credibly demonstrate respect for human rights;
- Provide individual users, investors, civil society advocates, and governments with information and criteria to make decisions about choices, strategies, and policy positions;
- Identify what specific legal and political factors prevent or hinder companies from respecting users' human rights.

This introductory section reviews how the business operations of Internet and telecommunications companies affect users' freedom of expression and privacy rights. Building on internationally established standards for business and human rights, we explain the role that we expect companies to play in mitigating those risks. We also lay the basis for the indicators on which we have evaluated the companies. The section then concludes with a general description of the methodology used to evaluate a set of 16 companies.

## 1.1 What and why

Internet and telecommunications companies commonly take the following actions, thus affecting their users' freedom of expression and privacy:

- Remove, block, or otherwise restrict content that users publish or share
- Block or shut down communications of certain people

---

4. United Nations, Human Rights Council Resolution, *The Promotion, Protection, and Enjoyment of Human Rights on the Internet*, A/HRC/RES/20/8 (July 16, 2012), [http://ap.ohchr.org/documents/dpage\\_e.aspx?si=A/HRC/RES/20/8](http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8).



- Shut down or otherwise restrict service to groups of people within a specific area or region (e.g., city, country)
- Share user information with third parties
- Collect and retain user information

Companies can take such actions for different reasons:

- **Government requests:** Around the world, government authorities and courts of law ask companies to take actions that affect users' freedom of expression and privacy. There are many legal reasons for such requests. For example, governments may ask companies to help identify individual users as part of a criminal investigation, or to restrict online content that violates local laws. However, when authorities abuse the government's power to make such requests, human rights violations can result: censorship of diverging opinions, blocking of communication channels, or the prosecution, persecution, and even killing of individuals who engage in speech and activities in accordance with their fundamental human rights.<sup>5</sup>

Certainly, freedom of expression and privacy are only two of many rights that citizens and technology users hold dear. Integrating essential objectives of freedom of expression, privacy, accountability, and security is not an easy task for companies or governments. In accordance with international human rights norms, governments are expected to protect human rights, and companies are expected to respect those rights.<sup>6</sup> In reality, however, companies in all countries where people use the Internet and mobile devices receive requests that arguably go beyond what can be considered "necessary and proportionate" to achieve other legitimate ends, and which therefore violate users' fundamental human rights.<sup>7</sup>

5. *Universal Declaration of Human Rights*, United Nations (1948) <http://www.un.org/en/documents/udhr/index.shtml> and *International Covenant on Civil and Political Rights*, United Nations General Assembly (1976) <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

6. U.N. Guiding Principles on Business and Human Rights, *op. cit.*

7. "Principles 3, 4, and 5: Necessity, Adequacy & Proportionality," in "Background and Supporting International Legal Analysis," *International Principles on the Application of Human Rights to Communications Surveillance*, (May 2014) <https://en.necessaryandproportionate.org/LegalAnalysis/principles-3-4-and-5-necessity-adequacy-proportionality>.

Intermediary liability – when the law holds companies responsible (liable) for users' actions and speech – creates challenges for companies that are committed to respecting users' rights.<sup>8</sup> Companies that operate under strict or ambiguous liability laws are often held responsible, either explicitly or implicitly, for policing hate speech or preventing terrorist activity in circumstances where the law does not clearly or narrowly define such speech and activities.

The findings of this Index highlight how laws and regulations may prevent companies from maximizing their respect for users' freedom of expression and privacy rights. However, we have also identified specific ways in which all companies are not as clear as they should be about how their compliance with laws and regulations can affect users' freedom of expression and privacy.

- **Private requests:** Private third parties – organizations or individuals not acting on behalf of a government entity – also ask companies to perform some or all of the actions listed above. Many private requests are made as part of processes sanctioned or stipulated by copyright and child protection laws. Other requests are made to companies through extralegal processes, including reporting mechanisms that companies create to receive requests and complaints about content or user behavior.

The Index identifies the extent to which the ranked companies inform users about the full range of private requests they receive, in addition to whether and how the companies respond to such requests. We identify specific ways that companies can improve their policies and practices to foster greater user trust and demonstrate that they are making maximum efforts to respect users' freedom of expression and privacy rights in the face of external demands.

- **Companies' own rules and processes:** Companies can also take action that affects users' freedom of expression and privacy for reasons unrelated to direct external requests. Through "terms of service," companies create their own rules that govern what types of content or activities are forbidden on their platforms. They set up their own systems and processes to enforce these rules. Enforcement can include deleting content, restricting access to the service, or shutting down accounts. The way companies enforce their rules can diminish users' freedom of expression.

8. *The Manila Principles on Intermediary Liability: Background Document*, Manilaprinciples.org, (May 2015) [https://www.eff.org/files/2015/07/08/manila\\_principles\\_background\\_paper.pdf](https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf).

- Company rules can also include requirements for how a user’s identity is publicly displayed, and what identity-related information the user is required to submit, either upon sign-up or during the course of enforcing identity policies. Enforcement of such policies can negatively affect users’ freedom of expression and privacy.
- **Handling of user information:** Companies collect, process, and retain user information for commercial purposes. They may also share this information with third parties for commercial or legal reasons. Once companies have collected that information, third parties can access it through commercial, legal or illicit channels. These include agreements between companies to share information, legal requests from governments, extralegal nation-state hacking, and even criminal attacks. By serving as a collection and storage point for user information, companies make themselves a target for compelled or covert data acquisition, making them responsible for keeping user data safe. Thus, due to the very nature of their businesses, ICT companies become guardians of essential human rights.

Rights, governments have the primary duty to protect human rights, but companies have a responsibility to respect human rights. Companies do not have direct control over the laws, regulations or other government actions of the countries where they operate. However, companies can carry out due diligence to anticipate potential human rights risks, and subsequently make informed business decisions on how to best prevent negative impacts on their stakeholders. In the context of Internet and telecommunications companies, this means that companies committed to respecting users’ rights should regularly assess how all aspects of their operations might potentially impact users’ freedom of expression and privacy. Companies also need to have clear processes and governance mechanisms in place to ensure that employees, managers, and executives at all levels are upholding and implementing the company’s commitments.

2. **Transparency and disclosure:** By disclosing as much information as possible about their policies and practices that affect users’ freedom of expression and privacy – including commercial data collection, enforcement of their terms of service, and compliance with government demands and legal requirements – companies can demonstrate a credible commitment to respect users’ rights. With sufficient information, people can better understand the risks they face and make informed decisions about how they use technology. People will also be in a better position to hold companies, governments, and other actors accountable for violations of their rights.

**Given the issues described above, Ranking Digital Rights expects companies to frame their commitments, policies, and practices around three core objectives:**

1. **Due diligence and governance:** According to the U.N. Guiding Principles on Business and Human

## User Information

Ranking Digital Rights applies the following definition of “user information:”\*

“User information is any data which is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques.”

Any data that documents a user’s characteristics and/or activities is therefore considered to be “user information.” This information may or may not be tied to a specific user account. It includes, but is 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 either through behavioral tracking or purchasing of data, and all forms of metadata.\*\* User Information is never considered anonymous except when included solely as a basis to generate aggregate measures (e.g. number of active monthly users). For further discussion of this definition and the project’s definition of “anonymous data,” please see Appendix 1 of the 2015 Research Indicators document.\*\*\*

\*. For more information, see Schwartz, Paul M. and Solove, Daniel J., “Reconciling Personal Information in the United States and European Union” (September 6, 2013) at: [http://papers.ssrn.com/sol3/papers.cfm?Abstract\\_id=2271442](http://papers.ssrn.com/sol3/papers.cfm?Abstract_id=2271442).

\*\* “A Guardian Guide to Your Metadata,” The Guardian, June 12, 2013, <http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1100110>.

\*\*\*. See <https://rankingdigitalrights.org/project-documents/2015-indicators/#appendix1>.

3. **Grievance and remedy:** According to the U.N. Guiding Principles, companies should establish a means of identifying and addressing any human rights violations or concerns that occur in relation to the company’s business. Internet and telecommunications companies should demonstrate that they have clear mechanisms in place for people to file grievances and receive remedy. Similarly, users must also have a way of learning about these mechanisms. In order for people to use such mechanisms appropriately and effectively, companies need to provide users with sufficient information not only about how companies receive and handle government requests, but also how companies handle non-governmental requests, how they collect, use, and share user information, and what the company’s own rules and enforcement processes are. This is one of many reasons why the Index places such great emphasis on transparency and disclosure.

Now that we have explained the basis on which the indicators used in the Index were formulated, the next section explains the research process and approach used to evaluate companies.

## 1.2 Our approach

Companies’ scores were generated through a rigorous multi-layered process that included primary research, peer review, company feedback, and quality control. The methodology used to evaluate the companies was developed over the course of three years, through a process of case study research, stakeholder consultation, and pilot testing. For a full description of this process, please see the project website at: [rankingdigitalrights.org/methodology-development](http://rankingdigitalrights.org/methodology-development).

**Companies:** Eight publicly listed Internet companies and eight publicly listed telecommunications companies were selected for review. This decision was based on several factors, including geographic reach and the diversity of markets in which the companies are headquartered and operating.

### Internet companies:

We examined company-wide policies and disclosure related to 2-3 selected services, as specified below.

- **Facebook, Inc.** (USA) – Facebook, WhatsApp, Instagram
- **Google, Inc.** (USA) – Search, Gmail, YouTube
- **Kakao Corp.** (South Korea) – Daum Search, Daum Mail, KakaoTalk

- **Mail.ru Group Ltd.** (Russia) – VKontakte, Mail, Mail.ru Agent
- **Microsoft Corp.** (USA) – Bing, Outlook.com, Skype
- **Tencent Holdings Ltd.** (China) – Qzone, QQ, WeChat
- **Twitter, Inc.** (USA) – Twitter, Vine
- **Yahoo! Inc.** (USA) – Mail, Flickr, Tumblr

### Telecommunications companies:

We examined disclosure at the parent-company level and for 1-2 selected services in each company’s home jurisdiction, as specified below.

- **América Móvil S.A.B. de CV** (Mexico) – Telcel’s mobile service
- **AT&T, Inc.** (USA) – mobile and fixed broadband service
- **Axiata Group Berhad** (Malaysia) – Celcom’s mobile service
- **Bharti Airtel Ltd.** (India) – mobile and fixed broadband service
- **Etisalat Group** (United Arab Emirates) – mobile and fixed broadband service
- **MTN Group Ltd.** (South Africa) – mobile service
- **Orange** (France) – mobile and fixed broadband service
- **Vodafone Group Plc** (United Kingdom) – mobile service

**Indicators:** Companies were evaluated on a total of 31 indicators, divided into three categories: Commitment (labeled “C”), Freedom of Expression (“F”), and Privacy (“P”).<sup>9</sup> A few specific indicators were only applicable to one type of company (Internet or telecommunications). Scores were based on companies’ performance across applicable indicators. See Section 4 of this report for further discussion of what was examined in each category, along with results and analysis.

**Scope:** This evaluation focused on companies’ publicly disclosed commitments, policies, and practices. We examined global commitments and disclosures at the highest corporate level of the company, as well as specific

9. Ranking Digital Rights, 2015 Indicators, [rankingdigitalrights.org/project-documents/2015-indicators](http://rankingdigitalrights.org/project-documents/2015-indicators).

policies and practices for selected services. For most indicators, news reports and other forms of secondhand disclosure were not considered in scoring (see the Appendix for further details). Information that was not publicly available was not considered in scoring, although we have included such information in the company reports (see Section 5) and other parts of this narrative. Most of the research and analysis was conducted between June 1, 2015 and July 31, 2015. The final cutoff date to consider any new disclosures was October 1, 2015. For further detail about the research and scope of evaluation, please see the project website or the Appendix of this report.

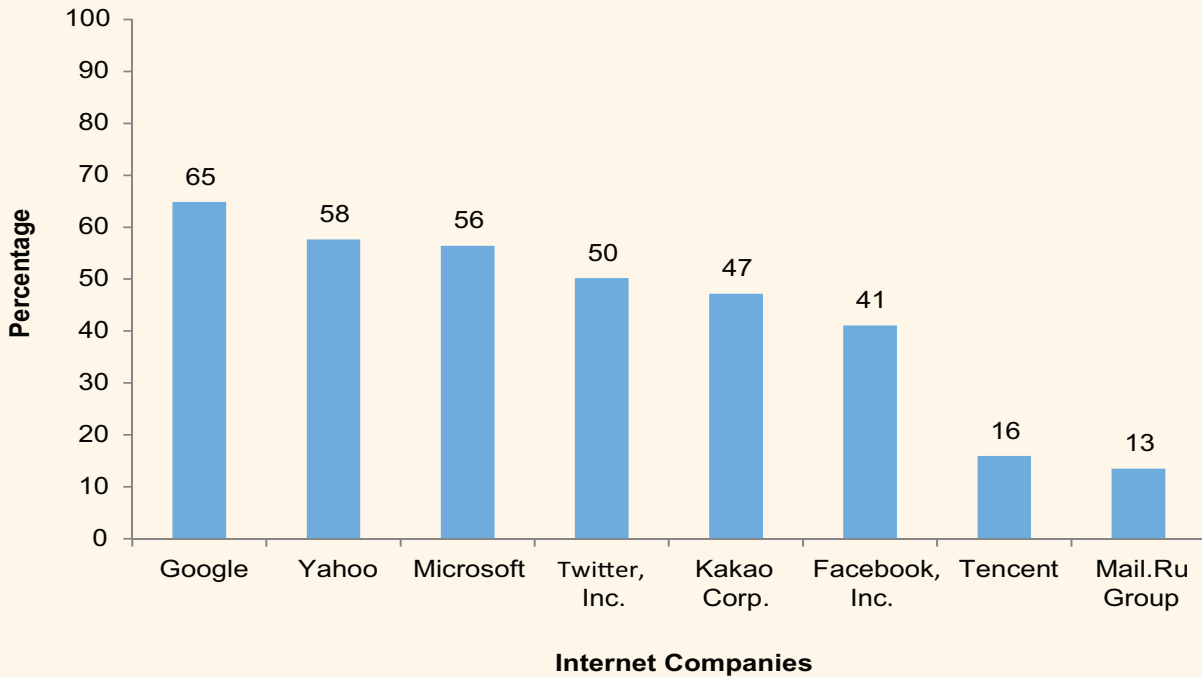
**Company engagement:** While company scores were based only on publicly available information, our team communicated with companies before and during our research. We sought feedback from companies while developing the methodology, and selected companies were notified of their inclusion in the Index when research began in June 2015. After our initial round of research and analysis, we contacted all 16 companies. We shared with them their draft results and invited them to provide feedback and any additional publicly available information that we might have missed. Nine of the sixteen companies chose to provide feedback, and we considered their feedback when determining final scores for each indicator.

**Analysis and data:** This narrative report contains our key findings and recommendations, analysis of company performance across categories, and individual company reports. The Appendix contains a table of company scores per indicator. To view comparative data for each individual company and indicator, or to download the raw data for each company and its component services, visit the project website at [rankingdigitalrights.org](http://rankingdigitalrights.org).

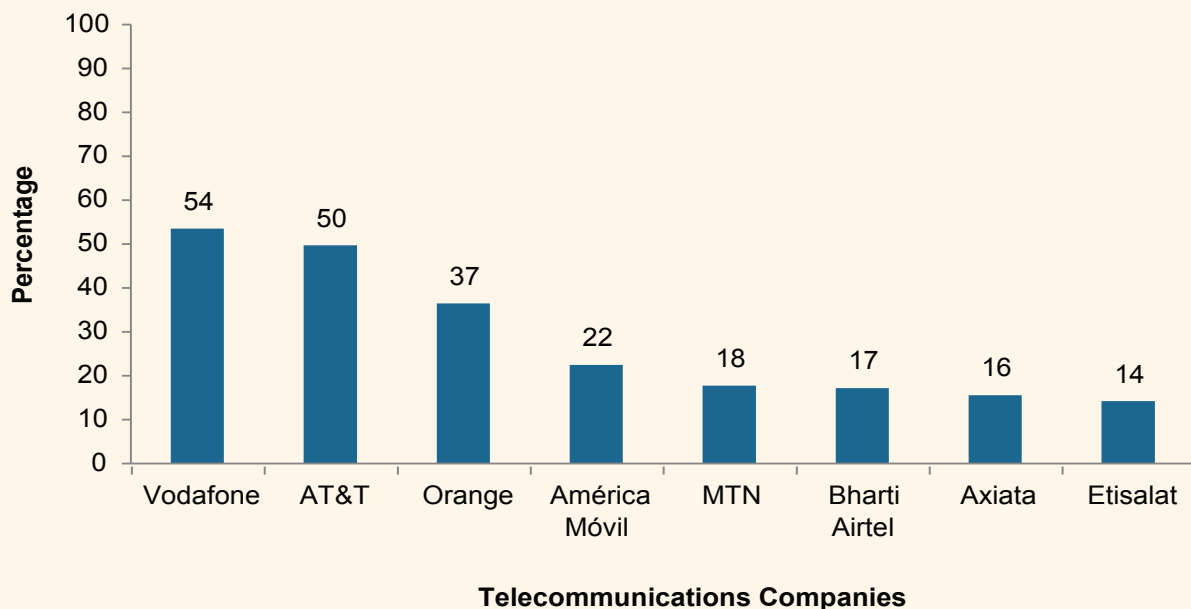
## 2. KEY FINDINGS

---

### Total Performance: Internet Companies



### Total Performance: Telecommunications Companies



**There are no “winners.” Even companies in the lead are falling short.**

Across the board, companies need to improve their commitments to, and disclosures of, policies and practices that affect users’ freedom of expression and privacy. The quality of companies’ disclosed policies and practices often fell short of stated commitments. There is much room for improvement even among companies that have made considerable – even laudable – efforts in certain areas.

No company in the Index provides users with sufficiently clear, comprehensive, and accessible information about the practices they have in place that affect freedom of expression and privacy. These include the handling of user information, terms of service enforcement, government requests and private requests.

**Nine companies can be considered to have made meaningful efforts to respect users’ rights.** However, companies’ efforts and disclosures were uneven and inadequate in many of their specifics. The top scoring company (Google) received 65 percent of the total possible score. Five other companies (Yahoo, Microsoft, Vodafone, Twitter, and AT&T) scored at least 50 percent. Three more (Kakao Corp, Facebook Inc., Orange) scored between 30-49 percent.

**Seven companies – nearly half – suffer from a serious deficit in respect for users’ freedom of expression and privacy.** América Móvil, MTN, Bharti Airtel, Tencent, Axiata, Etisalat, and Mail.ru scored between 13-22 percent. While some of these companies face substantial legal and regulatory obstacles to making commitments and disclosures related to freedom of expression and privacy in the jurisdictions where they are headquartered or operate, our research identified many indicators on which all companies in the bottom half of the Index can improve even if their legal and regulatory environments do not change.

**Despite Europe’s strong data protection laws, the two E.U.-based telecommunications companies were not Index leaders on disclosure of policies and practices related to the handling of user information.** Both Vodafone and Orange suffer from significant gaps in their public disclosures about the collection, retention, and sharing of user information. Surveillance and national security laws in those companies’ home countries are a substantial impediment to greater transparency about the volume and nature of government requests received to share user information. Nonetheless, our research identifies many areas in which these companies can improve, even without necessary legal reforms.

**Some Internet companies fail to effectively communicate key commitments, policies, and practices that are relevant to their users.** The best-performing Internet companies provided easily accessible

and well-organized privacy policies and terms of service, and they regularly published “transparency reports” that disclosed the frequency and nature of government and private requests. Some of the companies, despite making meaningful efforts to respect users’ rights, shared information about broader commitments, along with evidence for how those commitments are being implemented, through scattered tweets or blog posts, rather than offering a centralized overview of such information. By contrast, the telecommunications companies that performed best in the Index have clearly organized policy pages and documents on their own websites that are easy to locate and that articulate the company’s commitments and policies. Yet those companies suffer from significant gaps in disclosure.

**In sum, users are left in the dark about many company practices that affect freedom of expression and privacy.** Even for a very committed and concerned user who is willing to search news databases, pore over terms of service, and parse through privacy policies, it is impossible to formulate a clear picture about how the ranked companies’ practices may affect the user’s freedom of expression and privacy. Even our team of researchers, working full time for several months, struggled to draw definitive conclusions after evaluating many companies’ practices and policies – often times, because the relevant disclosures were disorganized, unclear, and sometimes even contradictory. In other cases, there were simply too many gaps in disclosure – or no disclosure at all – for entire categories of policy and practice. For further detail about individual company performance and analysis of trends, see Sections 4 and 5.

More specifically, the Index results point to some bad news as well as some good news when it comes to companies’ respect for users’ freedom of expression and privacy.

## **2.1. The bad news**

- **Disclosure about collection, use, sharing, and retention of user information is generally poor.** Even ranked companies that make efforts to publish such information are failing to communicate clearly with users about what information is collected about them, with whom it is shared, under what circumstances, and for how long they keep this information. This lack of clarity means that users, and especially at-risk users such as journalists, activists, or anyone living under a repressive regime, are not fully aware of who can access what specific information the company holds about them.

All companies except Orange and Mail.ru’s email and chat services make their privacy policies publicly available to people who have not signed up or subscribed. Nearly all companies take some steps to present these policies in a manner that

is easy for users to understand. However, even policies that are visually appealing and written in everyday language lack specificity, particularly related to what user information companies share and what control users have over their data. This is significant because it makes it more difficult for individuals to make decisions about information that is essentially private, and the sharing of such information risks enabling third parties to learn about their activities, interests, and connections. Please see Section 4.3 for more in-depth analysis

- **Disclosure about private requests to restrict content or share user information is minimal or ambiguous at best – and often non-existent.**

As described in Section 1.1, companies receive requests to restrict content or share user data from different types of third parties. In many cases these requests come from entities or individuals acting independently of any governmental authority, court, or judicial process.

As noted in the “good news” section below, companies are expanding disclosure and “transparency reporting” about government requests. Unfortunately, most companies’ disclosure does not include information about private third-party requests, even when those requests come with a court order or subpoena, or are made in accordance with established legal processes such as a copyright “notice and takedown” system. Even fewer companies disclose any information about whether – let alone the extent to which – they receive or respond to private or informal requests, which are requests to restrict content or share user information that are made outside of any official or legal process. While some companies told our researchers in private communications that they have no such disclosures because they have policies of never entertaining such requests, such requests do exist, and companies have failed to communicate relevant policies to users.

- **No company in the Index discloses any information whatsoever about the volume and type of user content that is deleted or blocked when enforcing its own terms of service.** As a result, indicator F9, which examines data about terms of service enforcement, was the only indicator in the entire Index on which every single company received zero points. Some companies objected to this indicator, arguing that such disclosure would be infeasible and counterproductive. Yet given the key role these companies play in facilitating the communication and expression of billions of people, their legitimacy as channels of expression hinges on how well they are governed. Without any insight into how companies implement their own terms of

service and other key policies, stakeholders have raised doubts about companies’ commitment to users’ freedom of expression.<sup>10</sup> Even if the most effective approach to greater transparency about terms of service enforcement has yet to be found, companies that face controversies surrounding their enforcement would be wise to take user concerns seriously.

- **Even if companies’ public disclosures may satisfy regulators, they omit information and context that users need.** A number of companies in the Index comply with privacy laws that impose requirements about, for example, what user information can be collected and retained under what circumstances. Other companies comply with laws that make it illegal to respond to requests not made through legally binding processes. Others comply with “net neutrality” regulations. Unfortunately, in a number of cases, these companies do not communicate with users about the legal framework in which they operate and how they are complying.

The lack of communication with users makes sense for a company that considers regulators, not users, to be its primary audience. It also makes sense if one expects users to be highly conversant in their home countries’ telecommunications and Internet related laws and regulations. However, it is our position that companies that seek to demonstrate respect for users’ rights should consider users as their primary – not secondary – audience in public communications about commitments, policies, and practices. It is reasonable to expect companies to provide basic disclosure about how they manage users’ private information, as well as access to information and communications flows, in the course of complying with laws.

- **Companies lack comprehensive grievance and remedy mechanisms.** In the Commitment category of the Index, we examined how companies approach mechanisms for stakeholders to report grievances, and what processes they have in place to offer meaningful remedy. (See Section 1.1 for discussion of remedy as a core element of companies’ respect for human rights.) We looked for easily accessible and readily displayed options for users to report concerns related to freedom of expression and privacy. Among the ranked companies, the tone of their existing disclosures did not suggest that improvement on the existing

---

10. See for example: Sahar Habib Ghazi, “How Indian Women Face Fatal Threats on Facebook While Trolls Run Free,” *Global Voices Advocacy*, August 6, 2015, <https://advox.globalvoices.org/2015/08/06/we-will-choke-you-how-indian-women-face-fatal-threats-on-facebook-while-trolls-roam-free/>.

communications avenues between the user and the company was a priority. Few companies met the expectations for remedy articulated by the U.N. Guiding Principles. This highlights a considerable gap between what service providers see as sufficient and what user advocates expect as best practice,<sup>11</sup> leaving much room for an open dialogue on what meaningful grievance and remedy practices for freedom of expression and privacy should look like. Notably, the company scoring highest points for remedy in the Index was Bharti Airtel of India, while the highest-scoring Internet company on remedy was Kakao of South Korea. In both cases these companies' strong performance is largely due to legal requirements in their home markets. For further discussion, see Section 4.1 and the individual company reports in Section 5.

- **The lack of end-to-end encryption makes private communications vulnerable to interception, sharing with third parties, and data breaches.** End-to-end encryption prevents even companies themselves from accessing the content of users' communications. With the exception of optional encryption on a messaging service of one company (Kakao), none of the ranked Internet companies offer end-to-end encryption by choice, let alone by default, for communications that users want to keep private and confidential.
- **In some instances, current laws and regulations make it more difficult for companies to respect freedom of expression and privacy. However, companies can still take actions to improve.** Some ranked companies are headquartered in countries whose laws and regulations governing Internet and telecommunications companies conflict with international human rights standards for freedom of expression and privacy. In most countries where the ranked companies operate, national security laws can forbid disclosure of certain types of government demands for user data, or other surveillance requirements. Some companies face more domestic, political, legal, and regulatory obstacles to respecting users' rights than others, because some countries' political and legal frameworks are less compatible with international human rights standards. Nonetheless, we have identified ways that *all* companies can improve their performance, even without changes to their political, legal, and regulatory environments. Please see the discussion of government requests and regulatory environments in Section 1.1 for further context, and see the company reports in Section 5 for concrete examples of specific companies in specific countries.

11. Peter Micek and Jeff Landale, *Forgotten Pillar: The Telco Remedy Plan*, Access Now, May 2013, [https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39\\_onm6ii982.pdf](https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_onm6ii982.pdf).

## 2.2 The good news

- **Corporate respect for freedom of expression and privacy is a global value.** While most of the companies demonstrating meaningful efforts are North American and European, one is from East Asia. The relatively strong performance of the South Korean company, Kakao, in this Index underscores how respect for freedom of expression and privacy has universal resonance.
- **Every company does something well.** Consider the following examples among companies whose overall scores totaled less than 25 percent: Bharti Airtel of India scored higher than other companies for its grievance and remedy mechanisms. Tencent of China publishes entertaining videos for users of its QQ messaging service about how to protect themselves against cyber threats. MTN, headquartered in South Africa with operations across Africa and the Middle East, has group-wide policy commitments to freedom of expression and privacy, and its board of directors has set up a committee to oversee these commitments. América Móvil, headquartered in Mexico, publicly commits to carry out due diligence on third-party requests for user information before deciding how to respond. The messaging service run by Mail.ru of Russia encrypts transmission of user communications by default. For more detailed company analysis, please see the company reports in Section 5.
- **"Transparency reporting" is becoming a standard practice.** Even since our research period ended, companies have continued to expand and improve the information they publish about third-party requests to restrict content or share user information. Nine of the 16 companies in the Index publish some form of "transparency report" that covers at least some types of third-party requests. However, there is wide variation in clarity, comprehensiveness, and quality of such reporting, and no company covers all types of third-party requests.<sup>12</sup> For more detail, see Section 4, of this report as well as the individual pages for indicators F7, F8, and P11 on the project website.
- **Nearly half of the ranked companies have backed up their commitments to freedom of expression and privacy by disclosing concrete measures they have taken to implement those commitments.** Seven companies in the Index

12. For recommendations directed at U.S. companies responding to law enforcement and government requests for user information, see Kevin Bankston, Ryan Budish and Liz Woolery, *The Transparency Reporting Toolkit and Research Memos*, Open Technology Institute, New America and the Berkman Center for Internet and Society, Harvard University, forthcoming November 2015 at: <https://www.newamerica.org/oti/transparency-toolkit/>.



earned more than 50 percent in the “Commitment” section. Notably, all of these seven companies are members of the Global Network Initiative (GNI), a multi-stakeholder initiative focused on upholding principles of freedom of expression and privacy in relation to government requests, or the Telecommunications Industry Dialogue, an industry organization also focused on freedom of expression and privacy. For further discussion of how participation in initiatives that are committed to upholding key human rights principles is proving to be an essential factor in companies’ articulation and implementation of commitments, please see Section 4.1.

- **All companies can improve their performance in the short to medium term, even without legal or regulatory changes.** See Section 3 for ways in which all companies can improve. Each company report in Section 5 also discusses how each company can improve, even without any changes to their broader legal and regulatory environments, market conditions, or business models.

# 3. RECOMMENDATIONS

This section lists key actions that companies, governments, and other stakeholders can take in order to maximize Internet and telecommunications companies' respect for users' freedom of expression and privacy.

## 3.1. For companies

Below are recommendations that apply to many companies in the Index.

Recommendations for specific companies can be found in the individual company reports in Section 5.

- **Communicate with users in a clear, accessible, and organized way.** Don't expect users to scour news archives, the blogosphere, and the Twittersphere in order to learn about the company's commitments and practices. Companies that are serious about demonstrating respect for users' rights – to their actual users and not just media elites or other specialized experts – should strive for well-organized disclosures in places that users can reasonably find.
- **Disclose and communicate what ordinary people – who aren't telecom lawyers or specialists in Internet regulation – need to know.** Companies should disclose and explain laws and regulations that affect users' freedom of expression and privacy. Companies should also disclose and explain how they comply with those laws and what that compliance means for users.
- **Conduct regular assessments to determine the impact of the company's products, services, and business operations on users' freedom of expression and privacy.** Several companies in the Index conduct different types of human rights impact assessments, a systematic approach to due diligence that enables companies to identify risks to users' freedom of expression and privacy as well as opportunities for companies to enhance users' enjoyment of those rights. While it would be counterproductive for companies to publish all details of their processes and findings, several companies in the Index have demonstrated that it is indeed possible to disclose information about a) the fact that the company conducts assessments and b) basic information about the scope, frequency, and use of these assessments.

For such disclosures to be credible, assessments should be conducted by an external third party which is accredited to a relevant and reputable human rights standard by an independent body whose own governance structure demonstrates strong commitment and accountability to human rights principles. As of 2015, only the Global Network Initiative meets the requirements for such an accrediting organization. For more details and resources related to human rights impact assessments and related assurance processes and bodies, please see Appendix 1 of the 2015 Research Indicators document<sup>13</sup> or the relevant resource pages on the project website.<sup>14</sup>

- **Disclose evidence that the company has institutionalized its commitments.** Even in cases where the research team happened to be personally familiar with the work of certain executives in particular companies, our methodology stipulated that companies could only receive credit if they provided publicly disclosed evidence that they have institutionalized their commitments with strong accountability and oversight mechanisms. While it is certainly important for a company to have leaders with strong personal commitments to users' rights, it is even more important that such commitments are clearly institutionalized. This bolsters external confidence that commitments may be honored and implemented even if those people leave the company.
- **Improve transparency and accountability about all types of third-party requests to restrict content or share user information.** To the maximum extent possible under the law, companies should publish comprehensive information related to the following types of third-party requests:
  - ▶ Process for responding to third-party requests to restrict content, access, or service (indicator F6)
  - ▶ Data about government requests to restrict content, access, or service (indicator F7)

13. See <https://rankingdigitalrights.org/project-documents/2015-indicators/#appendix1>.

14. See <https://rankingdigitalrights.org/project-documents/2015-indicators/#HRIA> and [https://rankingdigitalrights.org/resources/readings/samway\\_hria/](https://rankingdigitalrights.org/resources/readings/samway_hria/).

- ▶ Data about private requests for content restriction (indicator F8)
- ▶ Process for responding to third-party requests for user information (indicator P9)
- ▶ Data about third-party requests for user information (indicator P11)

See the individual indicator pages on the project website for full text of the indicators and their underlying elements.

If a company does not receive or entertain a particular type of request, the company should also clearly disclose that information.

- **Communicate clearly with users about what happens to their information.** If somebody were to create a dossier or “file” on the user based on what information the company holds at a given point in time, what would it look like? Companies should explain to users the lifecycle of information they collect. A user should understand:
  - ▶ What specific information the company collects (Indicator P3)
  - ▶ When or how the company collects that information (e.g., when the user registers for the service, when the user sends an SMS) (Indicator P3)
  - ▶ Whether users have an option not to provide that information (Indicator P5)
  - ▶ Specifically, what information the company shares and with whom (Indicator P4)
  - ▶ Why the company shares that information (Indicator P4)
  - ▶ Whether – and the extent to which – users can control the sharing of that information (Indicator P5)
  - ▶ How long the company retains that information (Indicator P7)
  - ▶ Whether the user can access that information (Indicator P6)
  - ▶ Whether and how the company destroys that information when users delete their accounts or cancel their service (Indicator P7)

See the individual indicator pages on the project website for full text of the indicators and their

underlying elements.

Many privacy policies discuss some of these practices, but often, the disclosure is too general to be meaningful. For example, a statement that a company stores personal information for as long as required by law or for as long as the company needs it provides no detail to users about the amount of time their information would reside in company servers. It also does not clarify whether the company stores different pieces of user information for different amounts of time. Framing company disclosure around how these practices apply to specific types of user information will give users a clearer and more comprehensive picture of how companies use their information.

- **Improve terms of service and privacy policies.** Indicators F1 and P1 examined whether terms of service and privacy policies are freely available and easy to understand. Companies that received full credit on these indicators did both, as well as provided their policies in languages commonly spoken by their users. In addition, companies should make sure they provide meaningful notice and documentation to users about changes to these policies.
- **Disclose meaningful amounts of information about the volume and nature of content and/or accounts restricted when enforcing terms of service.** The absence of any disclosures about restriction of content and accounts when enforcing companies’ terms of service undermines company commitments to respect users’ freedom of expression. While there are no clear answers regarding the optimal form of – and approach to – such disclosures, companies should engage with stakeholders to determine what types of disclosures related to terms of service enforcement would bolster trust and accountability.
- **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.
- **Communicate basic information about security practices and educate users about security threats.** Experts we consulted agree that it is reasonable to expect companies to implement

and disclose the measures described in indicators P12 (“Security standards”) and P14 (“Inform and educate users about potential threats”). Companies that are serious about maximizing users’ security should offer full encryption of user content, as described in indicator P13 (“Encryption of users’ private content”), for all relevant services in all possible legal contexts.

- **Implement end-to-end encryption to the greatest extent possible.** Such capabilities would go a long way to reassure users that their private communications are indeed safe from data breaches, interception, and sharing with third parties, and that it they will only be accessed by the desired recipients, now and in the future. At a minimum, companies should allow users to encrypt their own data.
- **Advocate for legal and regulatory changes that will support the company’s ability to respect users’ freedom of expression and privacy.** Our research has identified a number of ways in which the laws and regulations of particular countries prevent specific companies from performing as well as they otherwise might on certain indicators. We hope that our research findings can help companies work together with civil society advocates and responsible investors to make a convincing case for legal and regulatory reform that will maximize users’ enjoyment of their freedom of expression and privacy.

### 3.2. For governments

While companies have a responsibility to respect human rights, governments have a primary duty to protect human rights. Other projects such as Freedom House’s Freedom on the Net report<sup>15</sup> provide more specific measures of the extent to which governments are living up to their duty to protect Internet users’ rights. This Index data underscores the fact that governments create legal and regulatory environments that maximize companies’ ability to respect users’ rights. The following steps by governments would help companies in this Index to improve their performance:

- Legislative bodies and regulatory agencies should carry out their own impact assessments to ensure that laws and regulations governing Internet and telecommunications companies do not infringe on Internet users’ freedom of expression and privacy as defined by the Universal Declaration of Human Rights<sup>16</sup> and international human rights

15. See <https://freedomhouse.org/report-types/freedom-net> for the latest annual report.

16. Universal Declaration of Human Rights, *op. cit.*

instruments such as the International Covenant on Civil and Political Rights.<sup>17</sup>

- Legal liability imposed on companies for their users’ activities should be limited and consistent with the Manila Principles on Intermediary Liability,<sup>18</sup> a framework of baseline practices and standards to ensure that regulation of ICT sector companies does not result in the violation of users’ rights to freedom of expression and privacy.
- Surveillance-related laws and practices should be reformed to comply with the thirteen “Necessary and Proportionate<sup>19</sup>” principles, a framework for assessing whether current or proposed surveillance laws and practices are compatible with international human rights norms.
- Governments should publish their own transparency reports that disclose the volume, nature, and legal basis for requests made to companies.<sup>20</sup>
- Laws and regulations should allow companies to be transparent and accountable with users about how they receive and handle government requests
- Governments should develop effective data protection regimes and privacy regulations in consultation with industry and civil society, with impact assessments to ensure that the laws enacted can avoid unintended consequences for freedom of expression.
- In consultation with industry and civil society, legislatures should develop laws that require companies to implement effective mechanisms for grievance and redress when users believe that their freedom of expression and privacy rights have been violated while using companies’ services.

### 3.3 For all others: Individuals, advocates, activists, investors, and researchers

The data in this Index has many uses for individuals, consumer advocates, human rights activists, responsible investors, and researchers. In the months after launch, we will work with advocates, investors, and researchers to help them develop specific strategies for using the Index data. This work will be continuously documented on the

17. International Covenant on Civil and Political Rights, *op. cit.*

18. See <https://www.manilaprinciples.org/>.

19. See <https://en.necessaryandproportionate.org/>.

20. *Government Requests to Companies for User Information and Content Restriction: Transparency Policies and Practices*, Freedom Online Coalition Working Group on Privacy and Transparency Online, November 2, 2015, <https://www.freedomonlinecoalition.com/wp-content/uploads/2015/10/FOC-WG3-Privacy-and-Transparency-Online-Report-November-2015.pdf>.

project website. In the meantime, we have the following general suggestions:

- Encourage companies to improve everything over which they have meaningful control. The Index data includes many examples of good policy and practice and points to concrete ways in which practices could be improved.
- Use RDR's data as a starting point for more questions. These should be questions posed not only to and about the 16 companies included in the Index, but any other Internet or telecommunications company. Researchers may also use the indicators as the basis for sector- or topic-specific comparative studies.
- Work with allies within companies and governments wherever possible to change laws and regulations that prevent companies from respecting users' rights.
- Demand transparency and accountability of both companies and government actors regarding requests and expectations – legal and extralegal – being placed on companies. At present, no government provides meaningful transparency on requests made to companies. Citizens should push any government that is a signatory of the Open Government Partnership<sup>21</sup> and/or the Freedom Online Coalition<sup>22</sup> but does not release transparency reports about requests from authorities to companies for assistance with censorship and surveillance, to act in a manner more consistent with their commitments.

---

21. See <http://www.opengovpartnership.org/>.

22. See <https://www.freedomonlinecoalition.com/>.

# 4. CATEGORY ANALYSIS

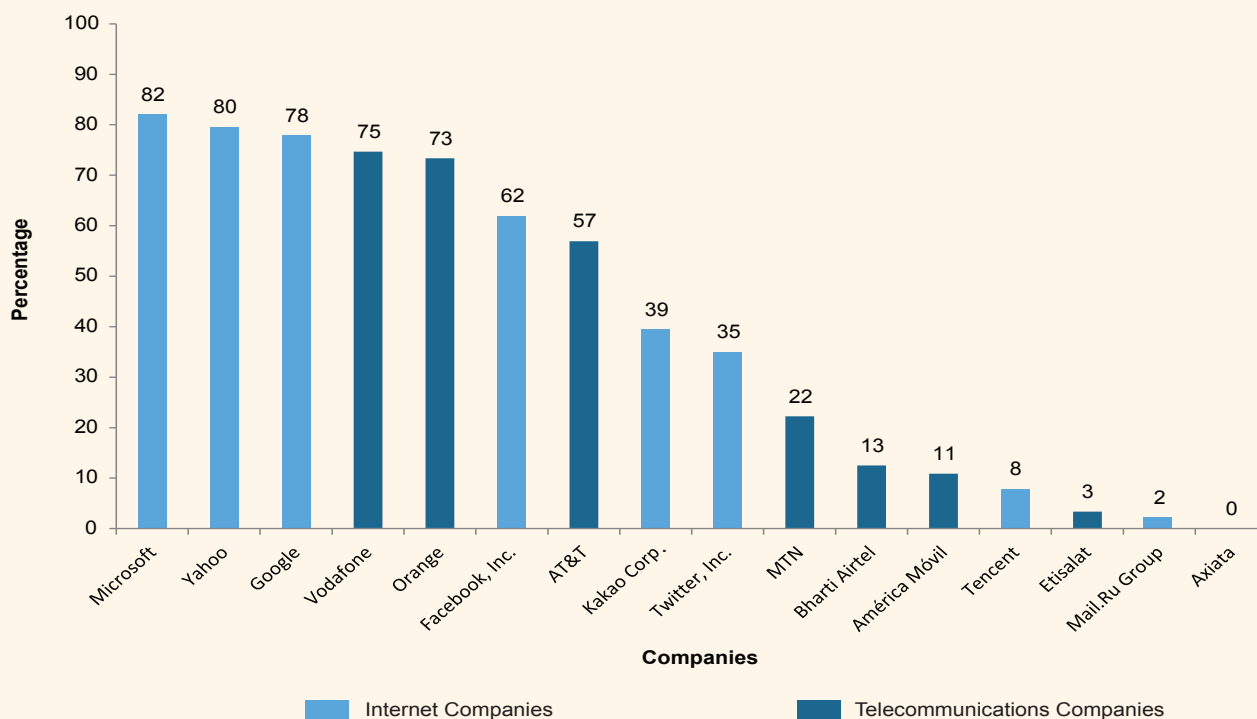
The methodology used to evaluate companies for the Index contained 31 indicators, divided into three categories: Commitment, Freedom of Expression, and Privacy.<sup>23</sup> This section explains what we examined in each category and provides in-depth analysis of key trends in company performance related to specific indicators within those three categories.

For more detailed analysis of individual companies' performance, please see the company reports in Section 5. To see data visualizations of performance on individual indicators, or to download the raw data, which includes scores and comments for every component of every indicator for every company, visit the project website at [rankingdigitalrights.org](http://rankingdigitalrights.org).

## 4.1. Commitment

The Commitment category of the Index evaluates whether companies demonstrate clear commitment in words and deeds to respect users' right to freedom of expression and privacy. The indicators draw heavily from the U.N. Guiding Principles on Business and Human Rights, which instruct companies not only to make commitments, but also to carry out due diligence – also known as “impact assessment” – in order to identify, mitigate, and account for any negative effects their business may have on human rights.<sup>24</sup> Companies are also expected to publicly demonstrate that they have put processes in place to implement their human rights commitments and policies effectively. Mechanisms for internal accountability, as well as grievance and remedy processes for users whose rights have been violated, are also important components of the Guiding Principles.

### Performance on Commitment



23. See <https://rankingdigitalrights.org/project-documents/2015-indicators>.

24. United Nations Guiding Principles on Business and Human Rights, *op cit.*, [http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

Microsoft, Yahoo, Google, Vodafone, and Orange take the lead (in that order) with Commitment scores between 70-82 percent of total possible points. Facebook, and AT&T fall within 50-65 percent. Kakao and Twitter trail in the 30-40 percent range; MTN, Bharti Airtel and América Móvil lag within the 10-25 percent band; and three companies (Tencent, Etisalat, and Mail.ru) are in the single digits. Axiata earned zero points for this section.

It is notable that the seven companies earning more than 50 percent of total possible points in this section are all members of the Global Network Initiative (GNI), a multi-stakeholder initiative focused on upholding principles of freedom of expression and privacy in relation to government requests<sup>25</sup> or the Telecommunications Industry Dialogue, an industry organization also focused on freedom of expression and privacy.<sup>26</sup> There is a close link between the commitments sought under the Commitment category and the principles that companies commit to as members of the GNI and Industry Dialogue:

- Members of the Industry Dialogue sign on to a set of “Guiding Principles” modeled on the U.N. Guiding Principles on Business and Human Rights, but tailored to telecommunications companies. They must report annually on their progress in implementing those principles. Companies that join the GNI commit to uphold a set of freedom of expression and privacy principles when faced with government demands to restrict speech or share user information.<sup>27</sup>
- The GNI Implementation Guidelines include due diligence processes as well as transparency and accountability mechanisms.<sup>28</sup> The 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.

However, the performance of GNI and Industry Dialogue member companies in this Index is not of uniform quality, as company scores across specific indicators clearly demonstrate. Among telecommunications companies, Vodafone and Orange’s commitments and disclosures were more comprehensive than those of AT&T.

Among Internet companies, Microsoft and Yahoo disclosed and articulated their commitments and

25. Global Network Initiative, <https://globalnetworkinitiative.org>.

26. Telecommunications Industry Dialogue, <http://www.telecomindustrydialogue.org/>.

27. See <http://globalnetworkinitiative.org/principles/index.php>.

28. See <http://globalnetworkinitiative.org/implementationguidelines/index.php>

practices in a clearer and more comprehensive manner than Google. Facebook’s lower score reflects the fact that it joined GNI in 2013, five years after the other three companies, which were founding members, joined in 2009. At the time of our research, Facebook had not yet completed a full GNI assessment. Also, many of Facebook’s disclosures and commitments do not appear to cover the company’s subsidiary acquired in 2014, WhatsApp.

**Grievance and Remedy.** On the question of grievance and remedy mechanisms, the Index results highlight how performance differs substantially from commitment and ideals. (See Sections 2 and 3 of this report for relevant key findings and recommendations.) The Global Network Initiative has stated its intention “to implement a standard for freedom of expression and privacy in the ICT sector that is consistent with the U.N.’s Protect, Respect, and Remedy framework.”<sup>29</sup> The Telecommunications Industry Dialogue, in its principles, has identified implementation of grievance mechanisms as an aspiration.<sup>30</sup>

However, unlike other indicators in the Commitment category, membership in the GNI or the Industry Dialogue was not a predictor of performance on indicator C6, which focused on grievance and remedy mechanisms that clearly include complaints related to freedom of expression and privacy. For instance, Bharti Airtel received the highest overall score on this indicator, beating out Vodafone, which also tied with América Móvil. Among Internet companies, Kakao led on remedy, edging out Google and substantially outperforming Microsoft, the Commitment category leader. The fact that few companies provided disclosure that aligned with expectations for business and human rights highlights an important opportunity for dialogue between industry and other stakeholders about what these practices should look like.

**Remedy standards:** In evaluating companies on their remedy and grievance mechanisms, we looked for companies to provide grievance mechanisms that were accessible and remedy standards that were clear.

In other words, we searched for tools that users could easily locate and understand in line with the Remedy section of the U.N. Guiding Principles. Beyond simple access to grievance mechanisms, the Index methodology gave credit to companies for disclosures about internal processes to investigate and resolve complaints, in addition to evidence that the stated mechanisms were implemented and operational. This included:

29. See <https://globalnetworkinitiative.org/content/frequently-asked-questions-about-gni-and-telecommunications-industry-dialogue>.

30. See <http://www.telecomindustrydialogue.org/overview-of-the-industry-dialogue/>.

- Clear articulation of the kinds of complaints companies were prepared to respond to, specifically including freedom of expression and privacy issues.
- Detail on the process for responding to complaints, such as how the company tracks complaints, which personnel are involved in responding to complaints, what procedures exist to escalate complaints, what timeline the company establishes for addressing complaints, what means the complainant has to follow up with the company, and what mechanisms exist for the complainant to appeal a decision.
- Some reporting on the number of complaints the company receives pertaining to freedom of expression and privacy.
- Some evidence and examples of complaints that were resolved. This last point is not meant to establish an expectation that all complaints and their resolutions become part of the public record. However, we expect that companies can provide insight into whether they are receiving and processing complaints and offer examples of issues and challenges that companies have considered and resolved.
- Bharti Airtel, the leader on this indicator across the entire Index, showed an alignment with Indian regulatory requirements that require grievance and remedy mechanisms for information technology and telecommunications companies. Of note, the requirements establish an expectation that companies implement a complaint monitoring system that enables the user to track the status of their case.
- In the case of Kakao, South Korean laws require implementation of grievance and remedy mechanisms that cover privacy and copyright. Our assessment determined that Kakao's performance largely aligned with regulatory expectations. Notably, Kakao has added an appeals mechanism for users who are accused of copyright infringement, which helps address concerns that processes for enforcing copyright can be used in a way that limits free expression.

While both of these companies can find considerable room to stretch toward the ideals that underpin the Index's methodology, their performance here provides a valuable example of how the regulatory context can support digital rights. There is further potential for stakeholders to work with regulators to close the gaps.

In all regards, company disclosures were evaluated with recognition that the privacy and safety of the complainants should be protected.

For telecommunications companies, many of the complaint avenues were embedded in terms of service or privacy policies. Internet companies tended to scatter the mechanisms across various web pages tied to specific functions of specific services. In many cases, locating the mechanisms and confirming whether they were relevant to our investigation represented a more complex journey than seemed reasonable for the average user. Much of the disclosure suggests that, even in spite of principled commitments, companies have not conceptualized how to incorporate grievance and remedy into their established communication mechanisms.

**Regulation and remedy:** While companies should voluntarily strive to implement policies that meet the standards of this indicator, regardless of regulatory requirements, evidence suggests that the strength of remedy practices to date is driven by the regulatory environment in companies' home countries. As previously mentioned, Bharti Airtel and Kakao displayed generally stronger performance on the assessment of grievance and remedy than other companies in the Index. Regulation appears to play a positive role: both India and South Korea have laws that require grievance and remedy mechanisms. (See the company reports in Section 5 for more detail.)

## 4.2 Freedom of Expression

This category examines the extent to which companies disclose concrete commitments and efforts to respect users' freedom of expression. Companies that perform well here demonstrate a strong public commitment to transparency, not only in terms of how they comply with laws and regulations or respond to government demands, but also how they determine, communicate, and enforce private rules and commercial practices that affect users' freedom of expression.

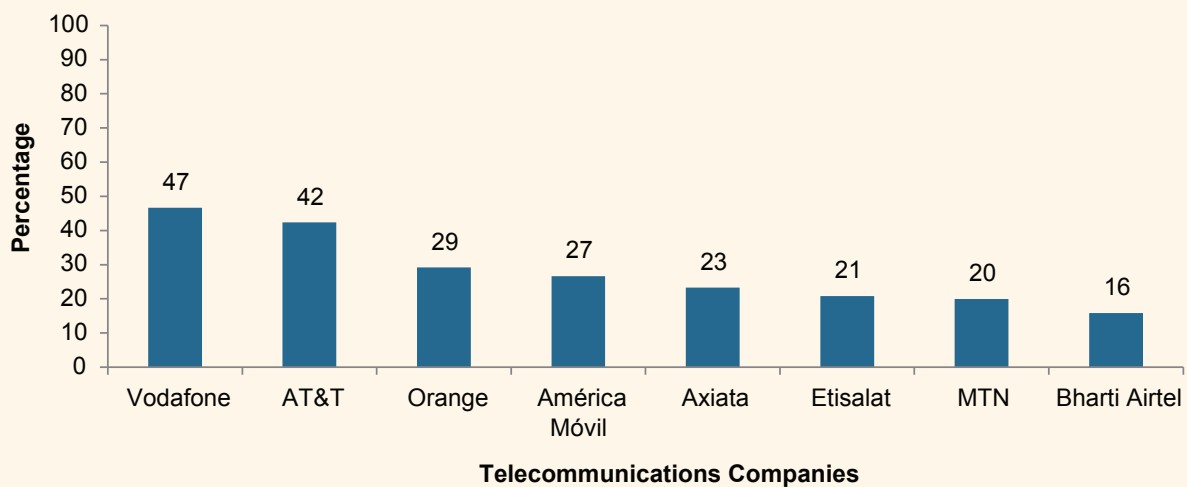
In this category, Internet companies generally received higher scores than telecommunications companies. This is due in part to the different nature of the services: telecommunications services are a conduit for speech and content, while Internet companies (among other functions) serve as a platform through which speech is shared publicly and privately. Internet companies everywhere impose restrictions on the activities and expression of users, either at the demand of private parties or through enforcement of their own terms of service. What is not universal is the extent to which they are transparent about these practices, and the extent to which these practices adhere to international human rights standards.

For telecommunications companies, the primary means of restricting user expression and access to information are the blocking or filtering of websites or network shutdowns in particular geographic areas. While such practices are



common in some jurisdictions, they are much less so in others. Nonetheless, there is a risk in all jurisdictions for telecommunications companies to infringe upon users' freedom of expression. Therefore, we take the position that assessing all telecommunications companies on freedom of expression criteria is appropriate and indeed necessary.

## Performance on Freedom of Expression: Telecommunications Companies

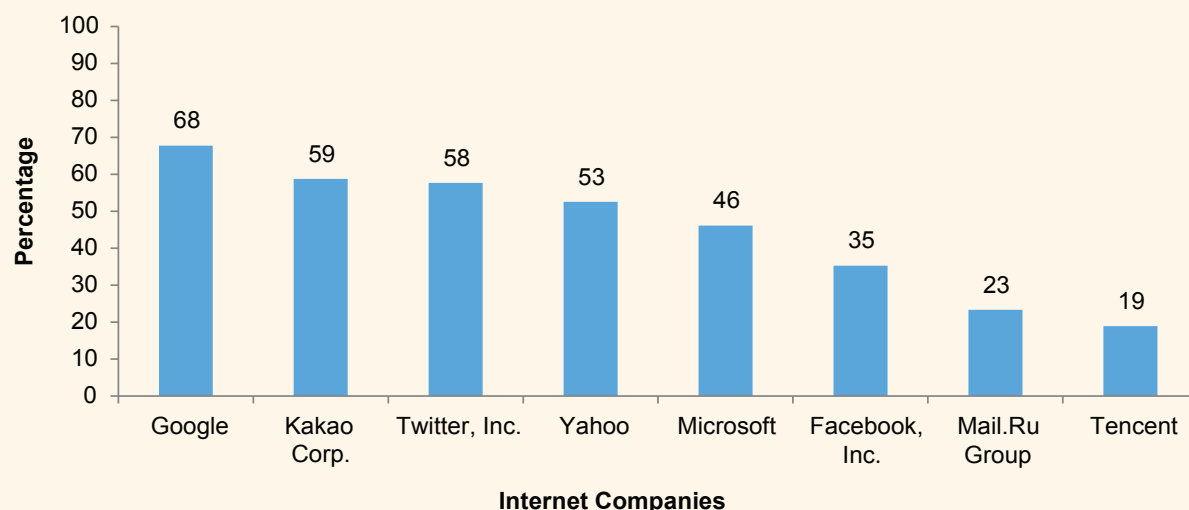


### Network Management

Indicator F10, which examined network management practices, applied only to telecommunications companies. It asks if a company *discloses* whether it prioritizes or degrades transmission or delivery of different types of content, and if so for what purpose. Effectively, it seeks disclosure on whether the company does or does not adhere to principles of net neutrality, and if not, why.

Of the eight telecommunications companies evaluated, only Vodafone disclosed that it does not prioritize or degrade the delivery of content (in the United Kingdom). Companies that provided no disclosure whatsoever for their home markets were Etisalat, MTN, and Orange. The others disclosed to varying extents that they prioritize or degrade content delivery in their home markets, and they explained their purpose for doing so (e.g., throttling speeds after users consume a certain amount of data).

## Performance on Freedom of Expression: Internet Companies



Among telecommunications companies, Vodafone was the relative leader on disclosed policies and practices that affect users' freedom of expression, although it received credit for less than 50 percent of the total possible score. It was followed by fellow Industry Dialogue member AT&T. Orange, the third Industry Dialogue member in the Index, followed distantly at 29 percent. The remaining companies ranged between 16-27 percent of total possible points.

Google's disclosed policies and practices that affect users' freedom of expression earned the company 68 percent of the possible total score, which is about ten percentage points higher than the next companies, Kakao and Twitter, who nearly tied at 59 percent and 58 percent, respectively. Yahoo earned slightly above 50 percent of total possible points for freedom of expression. Microsoft's lower score at 46 percent was due to the fact that until mid-October 2015, its transparency reporting did not include information about content restriction. On October 14, 2015, too late for inclusion in the Index, Microsoft published an updated version of its transparency report, which for the first time included data on content removal requests.<sup>31</sup> This disclosure will be evaluated in the next iteration of the Index.

31. John Frank, "New Transparency Hub debuts with latest reports," *Microsoft on the Issues* blog, October 14, 2015, <https://blogs.microsoft.com/on-the-issues/2015/10/14/new-transparency-hub-debuts-with-latest-reports/>.

Facebook's score was brought down by the lack of disclosure (and poorer quality of policies) for two of its services that are used by hundreds of millions of people around the world: Instagram and WhatsApp. (See Facebook's company report in Section 5 for more details.)

**Disclosure of rules:** Many, but not all, companies performed well on the indicator examining the availability of terms of service (Indicator F1). However, scores were much lower for indicator F2, which examines whether companies provide users with notice and a record of changes to those terms. This indicator expects companies to clearly commit to notify their users of changes to the terms of service and to maintain a log of those changes. Many companies objected to these expectations. Some argued that sending too many notifications to users and publishing archives of changes creates more confusion than clarity. Companies do not all agree, however. Kakao received perfect scores for two services, Daum Search and Daum Mail, on this indicator.

On two indicators in this category, all companies received at least some points, and companies that otherwise received low overall scores performed relatively well. Indicator F3 asks, "Does the company disclose whether it prohibits certain types of content or activities?" and indicator F4 asks, "Does the company explain the circumstances under which it may restrict or deny users from accessing the service?" The point of these indicators is that companies should be clear with users about what their rules are and how they enforce those rules. Interestingly, companies headquartered in countries

## Private Enforcement: The Black Box

Indicator F9 asks, “Does the company regularly publish information about the volume and nature of actions taken to enforce the company’s own terms of service?” As previously mentioned in Section 2.1 of this report, no company received any credit on this indicator.

Several companies told our researchers in private communications that publishing data about the volume and type of content removed in the course of enforcing terms of service (e.g., against hate speech, harassment, incitement to violence, sexually explicit content, etc.) would not, in their view, help promote freedom of expression. Some argued that too much transparency about such enforcement would enable criminals and people seeking to harm other users to more effectively “game” the system, while others argued that private enforcement also includes fighting spam, about which it supposedly would not be meaningful to provide insight.

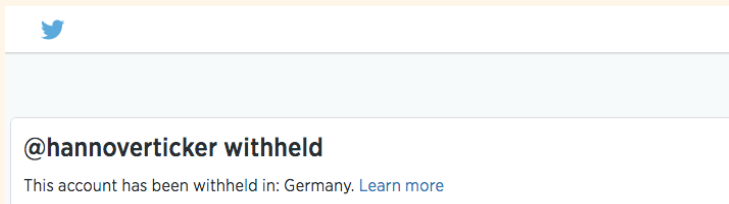
Yet at the same time, civil society groups in a range of countries have raised concerns that companies enforce their terms of service in a manner that is opaque and often viewed as unfair to certain groups.\* Such problems indicate that for companies to maintain or establish legitimacy as conduits for expression, they must also offer greater transparency and accountability in relation to how they police users’ content and activities.\*\* The score of zero across the board on this indicator highlights the need for dialogue among companies and other stakeholders about what reasonable steps companies can and should take to be more transparent and accountable about how they enforce their terms of service.

\* For example, see Michael Pizzi, “The Syrian Opposition is Disappearing from Facebook,” *The Atlantic*, February 4, 2014, <http://www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562>.

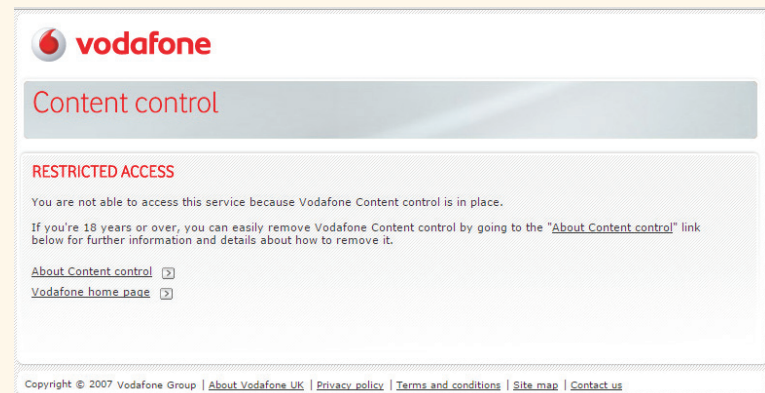
\*\* A project led by the Electronic Frontier Foundation was recently launched to call attention to this problem: <https://onlinecensorship.org/>.

where Internet censorship is documented to be relatively extensive tended to score fairly well on these indicators – presumably due to their need to demonstrate compliance with legal restrictions on speech. For more information, see the company reports in Section 5 as well as the company and indicator pages on the project website.

**Notifying users of restrictions:** Indicator F5 asks, “If the company restricts content or access, does it disclose how it notifies users?” The indicator seeks company commitments to notify users who are blocked from accessing all or part of a service, are blocked from viewing content, or when they are trying to view content that has been removed from the service entirely. To receive credit on this indicator, such disclosure must be accessible to people who are not signed up or subscribed to the service. Twitter, for example, explains how it notifies users when they are prevented from viewing “country withheld content.” (See screenshot below).



Other companies do not provide any publicly available commitments or disclose materials about how or under what circumstances they notify users, although users have reported receiving notifications from companies when trying to access blocked content. (See screenshot below).



One company, for example, suggested to our researchers that we should find a subscriber of their service and ask the person to access a particular website that the company blocks in order to verify that they do notify users. As previously mentioned, the Index methodology does not consider information that can only be verified by paying subscribers when giving credit. It is important that companies publicly disclose information about

their policies and processes for notifying users about content and access restrictions. Such disclosure will improve accountability around how content and access restrictions are implemented. This practice not only enables stakeholders who are not subscribers to evaluate and compare among different companies' practices, it also gives consumers an opportunity to make informed decisions about how different companies communicate with users about restrictions.

**Transparency reporting:** Fewer companies publish disclosures about third-party requests to restrict content – a key area examined in the Freedom of Expression category – than publish disclosures about requests to share user information (see Section 4.3). While 11 companies disclosed some information about their process for responding to government requests for user data (see the discussion of Indicator P9 in Section 4.3), only eight disclosed information about their process for responding to content restriction requests made by government or court authority (Indicator F6). Nine of the ranked companies published data about government requests for user information (see the discussion of Indicator P11 Section 4.3), but only six (AT&T, Facebook, Google, Kakao, Twitter, and Yahoo) published data about government requests to remove user content (Indicator F7). Of those, only four (Google, Kakao, Twitter, and Yahoo) disclosed any data related to requests made

by private entities not acting on government or court authority (Indicator F8).

Notably, two companies go beyond the reporting of numbers and enlist the help of a non-profit project to publish the text of at least some of the content restriction requests that they receive. Founded in 2001, the Chilling Effects database hosted by Harvard's Berkman Center for Internet and Society collects and analyzes legal complaints and requests for removal of online materials.<sup>32</sup> In 2002, Google started submitting content removal requests that it receives from copyright holders.<sup>33</sup> Since then, several other companies including Twitter have chosen to use the project as a neutral third-party host for takedown requests received around the world.<sup>34</sup>

## Identity Policies

Indicator F11, which applied only to Internet companies, asks, "Does the company require users to verify their identity with government-issued identification, or with other forms of identification connected to their offline identity?" The answer "no" received full points and the answer "yes" received zero points. Google, Microsoft, Twitter, and Yahoo scored full points on this indicator. Facebook and Mail.ru both scored 67 percent. While Facebook's Instagram photo sharing service and WhatsApp messaging application can be used without users having to share their real names, its namesake Facebook network has a "real name" policy that requires users to provide, upon request, forms of identity that can be connected to their government ID. Mail.ru's VKontakte service maintains a similar requirement. Kakao received a 50 percent score due to vagueness in its policies about the circumstances and methods by which the company might seek to verify a user's identity. Tencent received zero points due to strong "real name" policies for all services. For more information about how strict enforcement of "real name" policies can stifle freedom of expression please see the Open Letter to Facebook published by a coalition of non-governmental organizations representing individuals who have experienced harm as a result of such policies.\*

\* "Open Letter: Facebook Must Change Its Broken "Real Name" Policy," *Global Voices Advocacy*, October 5, 2015, <https://advox.globalvoices.org/2015/10/05/open-letter-facebook-must-change-its-broken-real-name-policy>.

32. Chilling Effects website: <https://www.chillingeffects.org>.

33. See for example DtecNet DMCA (Copyright) Complaint to Google, Chilling Effects Clearinghouse, March 12, 2013. [www.chillingeffects.org/notice.cgi?SID=841442](http://www.chillingeffects.org/notice.cgi?SID=841442).

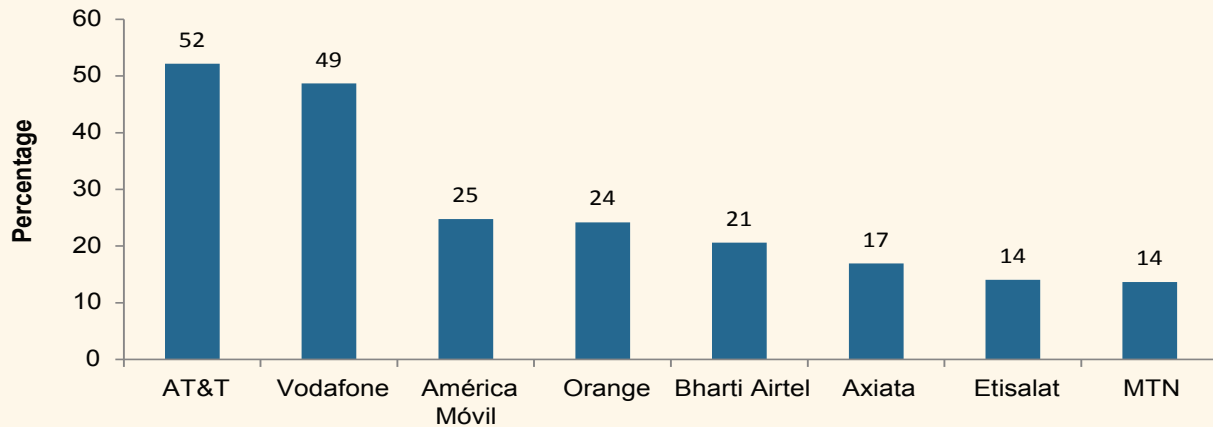
34. "About," Chilling Effects, <https://www.chillingeffects.org/pages/about>; and "Huge Volume Increases and Updates to Google Transparency Report," *Chilling Effects Blog*, 13 December 2012. [https://www.chillingeffects.org/blog\\_entries/585](https://www.chillingeffects.org/blog_entries/585).

### 4.3. Privacy

This category examines whether companies' commitments and disclosures demonstrate credible efforts to respect users' right to privacy. Companies that performed well in this category showed a strong public commitment to transparency, not only in terms of how they respond to government demands, but also how they determine, communicate, and enforce terms of service and commercial practices that affect users' privacy. Commitments to protect and defend users' digital security are also an important component of this category.

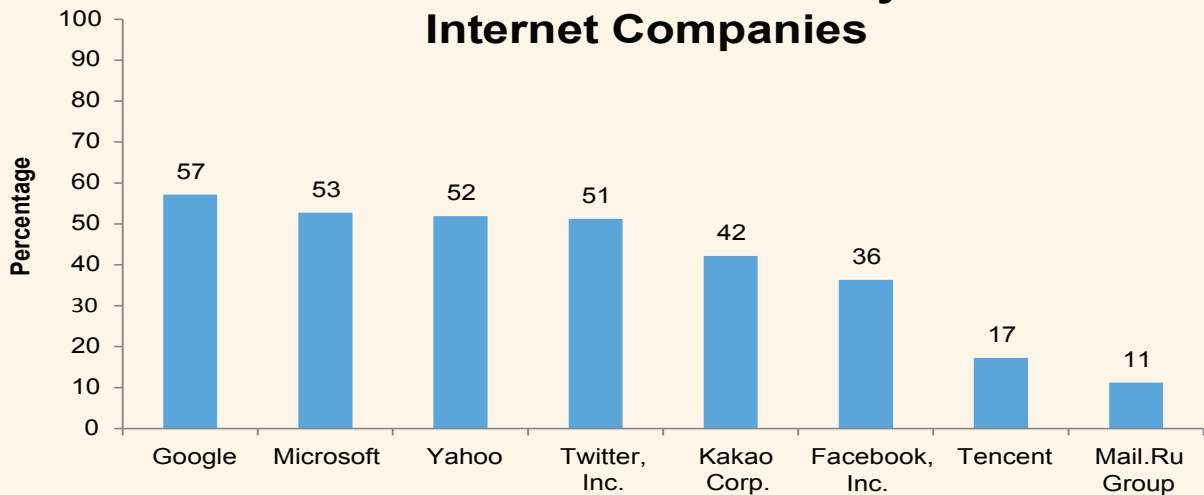
AT&T and Vodafone were the clear leaders among telecommunications companies, earning 52 and 49 percent, respectively, of the total possible points on disclosure of policies and practices that affect users' privacy. (See the company reports in Section 5 of this report and on the project website for further discussion of the factors that contributed to both companies' scores.) América Móvil, Orange, and Bharti Airtel came in a band of scores between 21-25 percent. Axiata, Etisalat, and MTN followed with scores in the mid-teens.

### Performance on Privacy: Telecommunications Companies



Telecommunications Companies

### Performance on Privacy: Internet Companies



Internet Companies

The top four Internet companies, Google, Microsoft, Yahoo, and Twitter scored more than 50 percent of total possible points, with scores ranging between 51-57 percent. They were followed by Kakao at 42 percent and Facebook at 36 percent. Facebook's score on privacy was affected by the same factors that influenced its Freedom of Expression category score: lack of strong policy and disclosure for Instagram and WhatsApp in contrast to the stronger performance of the Facebook service itself. Tencent and Mail.ru trailed distantly.

**Disclosures to users about company handling of their information:** As we previously noted in Sections 2 and 3 above, our research found industry-wide incoherence in disclosures to users about how companies handle their information: what is collected, how it is collected, how long it is retained, and with whom it is shared.

Nearly all companies made some effort to help users understand their privacy policies, for example, by writing them in plain language or using section headers and bulleted lists to help users absorb the information. Despite this, companies failed to provide a clear picture of how they handle user information. As explained in Section 1.1, this project takes an expansive interpretation of "user information," defining it as "any data that is connected to an identifiable person, or may be connected to such a person by combining datasets or utilizing data-mining techniques."<sup>35</sup>

All companies provided at least some explanation about the information they collect from users (Indicator P3). Kakao was the only company that explicitly commits to data minimization: limiting collection of user information to what is directly relevant and necessary to accomplish the purpose of its service. While other companies may adhere to legal requirements for data minimization, their own disclosures to users do not clearly mention it.

All companies also disclosed some information about what they share with third parties (Indicator P4), though companies performed significantly worse in disclosures about sharing than collecting. In part, this stemmed from the use of varied terms related to user information, including "personal information," "personal data," "private personal information," "sensitive personal information," or "anonymous information." Even when policies defined these terms, it remained unclear what types of user information these terms did or did not include. For example, if a company stated it does not share personal information with third parties, but its definition of "personal information" only included items such as name and email address, it remained unclear whether the company shared log data or location data with third parties.

Debates about what constitutes private, personal, sensitive, or anonymous information are far from settled, particularly given the continuous advancement of data analysis techniques that can combine information in unpredictable ways. Nevertheless, if companies more clearly explain how they handle the different types of information they collect, users can make more informed choices about whom to entrust with their data.

No company clearly explained whether users can control what the company itself collects and shares about users (Indicator P5). While six companies allow users to opt-out of the sharing of their information for either app integration or analytics purposes, users are left wondering whether this is the only say they have in how their data is shared. Furthermore, half of the companies did not explain whether users can access the information the company holds on them (Indicator P6), and seven companies did not provide detail on how long they hold user information (Indicator P7).

As noted previously, despite the European Union's strong data protection laws, the two E.U.-based companies in the Index were not the top performers on indicators examining *company disclosure* about collection, retention, and sharing of user information. For example, on indicator P4, which asks whether companies disclose if and why they share user information with third parties, Orange and Vodafone disclosed less information than AT&T and several U.S.-based Internet companies. On indicator P7, which examines whether companies disclose to users how long they retain user information, Orange received no credit (along with AT&T), while Vodafone's score was lower than several U.S.-based Internet companies.

While Europe-based companies may be communicating with regulators on such matters in order to ensure compliance with the law, they do not communicate so well with users – at least those who are not conversant in telecommunications and privacy law. In Sections 2 and 3 above, we discussed the reasons why, from a human rights perspective, it is insufficient for companies to communicate with regulators but not communicate clearly with users about what happens to their information.

Internet companies were also evaluated on disclosure about whether and how they collect user information from other services and websites (Indicator P8). Such disclosure helps users understand how their online activities outside a company's services, tracked through "cookies" and other web-tracking mechanisms, might affect their use of those services. Facebook, Inc. and Google scored very poorly on this indicator (in the single digits for each company), while Microsoft and Yahoo had

---

35. See <https://rankingdigitalrights.org/project-documents/2015-indicators/#userinformation>.

somewhat more disclosure.<sup>36</sup> Twitter was the clear leader on this indicator: It was the only company in the Index to support the “Do Not Track” standard<sup>37</sup> that allows users to opt-out of certain types of web tracking. All other Internet companies had no disclosure whatsoever about whether they collect user information from third parties.

**Legal obstacles to transparency about government requests:** Three indicators in the Privacy category focus on ways that companies can be transparent about third-party requests for user information. Specifically, the indicators focus on company processes for responding to third-party requests for user information (P9), user notification about third-party requests for user information (P10), and data about third-party requests for user information (P11). All companies face varying legal barriers – primarily national security and secrecy laws – that make perfect scores on these three indicators difficult in some cases.

On indicator P9, which examines companies’ disclosure of processes to respond to government or other third-party requests for user information, the highest-scoring companies in the Index are headquartered in countries where the law is not an obstacle to disclosing basic information about such processes. However, in other countries, the law may be interpreted as potentially preventing disclosure about at least some types of processes (see the company report in Section 5 or on the project website for the French company Orange, which received a zero score on Indicator P9). In yet other countries, such as South Africa, the law forbids disclosure of the fact that the government has made any request for user information. If MTN, the South African company in this Index, published its process for handling South African government requests, it would acknowledge the existence of such requests, and thus violate the law.<sup>38</sup> In China, where Tencent is headquartered, a company could be found in violation of national security and state secrets laws for disclosing how it receives and responds to requests.<sup>39</sup>

The laws of many countries restrict the circumstances under which companies can notify users about government requests for user information.

---

36. For full set of elements in this indicator see [rankingdigitalrights.org/project-documents/2015-indicators/#P8](http://rankingdigitalrights.org/project-documents/2015-indicators/#P8); For a definition of “user generated signals” used in this indicator see [rankingdigitalrights.org/project-documents/2015-indicators/#usergenerated](http://rankingdigitalrights.org/project-documents/2015-indicators/#usergenerated).

37. See <http://donottrack.us/>

38. Charlie Fripp, “SA phone companies may be used for spying, but can’t tell you when,” *htxt.africa*, June 6, 2014, <http://www.htxt.co.za/2014/06/06/sa-phone-companies-may-be-used-for-spying-but-cant-tell-you-when/>.

39. Sky Canaves, “Beijing Revises Law on State Secrets,” *The Wall Street Journal*, April 29, 2010, <http://www.wsj.com/articles/SB10001424052748703572504575213944098022692>.

No telecommunications company from any country received any score on indicator P10, which asks whether the company notifies users about any type of third-party request for user information. However, most services of all U.S.-based Internet companies received credit for committing to notify users when government entities (including courts or other judicial bodies) request their user data. Many also received credit for disclosing situations when the company might not notify users, including a description of the types of government requests they are prohibited by law from disclosing to users.

On Indicator P11, which examines whether the company publishes data about government and other third-party requests for user information, the U.S.-based companies (except Facebook) and Kakao of Korea scored substantially higher than the only two other companies that received any score for this indicator, Orange and Vodafone (both with 35 percent). The U.S.-based companies report on the number of requests received, while the two European telecommunications companies provide more general information. Vodafone cites the law as a barrier to publishing further detail. (See company report in Section 5 for more details.) As for companies that scored no points for this indicator, some, like MTN in South Africa, face clear legal prohibitions against reporting on government requests for user information. However, for América Móvil in Mexico, the law does not impose the same limitations.

The individual company reports in Section 5 and on the project website contain more details about the specific legal contexts in which each company operates.

Laws in many countries prevent companies from disclosing information about at least some types of government requests, and thus cause the companies’ Index scores to be lower. In fact, some stakeholders even in very open societies argue that, for security and law enforcement reasons, it is not desirable for companies to be fully transparent about all types of government requests. Nonetheless, we believe that our strict approach to scoring of these indicators offers a framework for necessary debate among stakeholders about what prohibitions on disclosure are truly necessary in societies committed to integrating security-related concerns and practices with international human rights standards.

In some countries, laws barring disclosure of requests to companies for user information also cover some categories of court orders. In many countries, the laws are not clear about what types of processes and requests a company can in fact legally disclose.

Companies everywhere indicate that they must err on the side of caution in order to protect their employees from prosecution.<sup>40</sup>

Our results on these indicators highlight the need for legal reforms that clarify what companies can and cannot disclose before, during, and after the fact. Prohibitions around disclosure should be limited to very narrow circumstances.<sup>41</sup> Furthermore, there are no compelling reasons why companies should not be allowed – by governments claiming to be committed to public accountability – to inform users at very least about the *types* of requests they are prohibited from disclosing.

**Lack of transparency about private requests:** Indicators P9, P10, and P11 (discussed above) all contained elements that examined disclosures about private requests, in addition to government requests whose disclosure can be legally problematic in some places and contexts. While laws of confidence may bar companies from disclosing information about specific requests, no companies face direct legal prohibitions against general descriptions of their processes for responding to requests for user information made by private parties, although some are deterred by legal ambiguity or weak rule of law. In some jurisdictions, the lines between public and private are blurry. In China, for example, government officials are known to make demands via private channels such as mobile phone text messages to company employees who understand that there will be consequences if they refuse.<sup>42</sup> In such jurisdictions, it may be unrealistic to expect corporate transparency about most types of third-party requests without placing individual employees at risk until legal mechanisms to prevent abuse of government power are strengthened.

In many other jurisdictions where due process and rule of law are clearer – in other words, in countries where it is possible for companies to challenge government authorities in court, and for individuals to challenge companies as well as governments – the legal experts we consulted could identify no reason why companies cannot or should not disclose their policies and practices for handling private requests, as well as data about the numbers of private requests they receive.

In the U.S., while the law restricts companies from providing the content of users' communications to third parties, it does not prevent the sharing of some other

types of user information with non-governmental third parties.<sup>43</sup> At least a few such requests have apparently occurred: there are documented cases of intellectual property owners and defamation claimants trying to address concerns about infringement who have requested the information about domain name registrants that use privacy and proxy services to keep their personal data out of ICANN's WHOIS database.<sup>44</sup> Therefore it is reasonable to expect a company to clarify and disclose whether it accepts or responds to private requests for certain types of information pertaining to users. U.S. companies that disclose such information include Tumblr (owned by Yahoo).<sup>45</sup>

Our methodology thus takes the position that companies who have a policy not to accept private requests made without any legal authority have an obligation to clearly inform users of their commitments, policies, and practices surrounding such types of requests, as they pertain to different types of user information.

For this reason, companies that make no public disclosures about private requests for user information – whether or not they actually receive or comply with such requests – lost points in our three indicators focused on third-party requests. Some of these companies made assurances in conversations with our researchers that they indeed have policies not to accept or comply with private requests for user information. If these companies clearly disclose such commitments and policies to users in future, their scores can easily increase on several relevant indicators in future iterations of the Index.

For Indicator P9, only one service of one company, Tumblr (acquired by Yahoo in 2013), provided disclosure that clearly states that it does not entertain requests without a valid subpoena, search warrant, or other government order. All other companies were too vague in their disclosure to receive credit on elements examining private requests not only in P9 but also P10 and P11.

**Security standards:** Indicator P12 examines several security-related aspects of companies' disclosure, including whether they conduct security audits, keep up with latest encryption standards and have systems in place to limit employees' access to user information. The indicator applied six different elements for Internet

40. See for example Vodafone Law Enforcement Disclosure Report 2015, p.3. [http://www.vodafone.com/content/dam/sustainability/vodafone\\_law\\_enforcement\\_disclosure\\_report\\_2015.pdf](http://www.vodafone.com/content/dam/sustainability/vodafone_law_enforcement_disclosure_report_2015.pdf).

41. User notification. International Principles on the Application of Human Rights to Communications Surveillance, Necessary and Proportionate Principles, May 2014 [https://en.necessaryandproportionate.org/text#principle\\_8](https://en.necessaryandproportionate.org/text#principle_8).

42. "China," *Freedom on the Net 2014*, Freedom House, <https://freedomhouse.org/report/freedom-net/2014/china>.

43. <https://www.law.cornell.edu/uscode/text/18/2702>.

44. For example see <http://www.bailii.org/ew/cases/EWHC/QB/2015/2628.html> and Jeremy Malcolm & Mitch Stoltz, "Changes to Domain Name Rules Place User Privacy in Jeopardy,"

*Electronic Frontier Foundation*, June 23, 2015, <https://www.eff.org/deeplinks/2015/06/changes-domain-name-rules-place-user-privacy-jeopardy>.

45. <https://wiki.sonic.net/wiki/Category:Policies#Privacy>; "Law Enforcement Guidelines," CREDO Mobile, <http://www.credomobile.com/law-enforcement-guidelines>.; "2014 Transparency Report," Dropbox, <https://www.dropbox.com/transparency>.



companies and four elements for telecommunications companies. (See the indicator page on the project website for full details.) Two telecommunications companies earned full scores: AT&T and Vodafone. Orange came in third, Kakao fourth and Google fifth. Other companies that earned at least 50 percent of total possible points on this indicator were Yahoo, Microsoft, Bharti Airtel and Twitter. Several more companies earned between 10-40 percent: Facebook, Mail.ru, América Móvil, Axiata, and MTN. Etisalat and Tencent received zero points.

**Security education:** Indicator P14 examines whether a company publishes information to help users defend against cyber threats. A number of companies received full scores: América Móvil, AT&T, Bharti Airtel, Google, Orange, and Vodafone. It is clear to our researchers and consulted legal experts that there is no reason why all companies should not be able to earn full scores on this indicator.

**Encryption of users' content:** Indicator P13 applied only to Internet companies. Companies could only receive full credit if private user content is encrypted end-to-end by default – in other words, the company itself has no access to the content itself, or to the encryption keys needed to decrypt it. This indicator obviously does not apply to social media features through which users intentionally share content with large groups, or publicly. It does apply to services such as email, chat, and other private messaging offered by Internet companies, sometimes even in conjunction with public-facing social media platforms. No company in this year's Index received a full score on this indicator, and only one company (Kakao for its messaging service KakaoTalk) received partial credit for its optional encryption feature.

Even in countries where the Internet is considered relatively free, as of November 2015, legislation is being proposed to outlaw such encryption. For example, British Prime Minister David Cameron has been calling for a ban on encryption that is impenetrable to anyone but the end user,<sup>46</sup> as has U.S. Federal Bureau of Investigation director James Comey.<sup>47</sup> The overwhelming consensus among computer security experts is that encryption that contains a so-called “backdoor” is no encryption at all.<sup>48</sup>

---

46. Price, R. (2015, July 1). David Cameron is going to try and ban encryption in Britain. Business Insider. Retrieved from <http://www.businessinsider.com/david-cameron-encryption-back-doors-iphone-whatsapp-2015-7>.

47. Comey, J. (2014, October 16). Going dark: are technology, privacy, and public safety on a collision course?. Brookings Institution, Washington, DC. Retrieved from <http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

48. See Abelson, H. H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W. W., ... & Weitzner, D. J. (2015). Keys under doormats. *Communications of the ACM*, 58(10), 24-26. Available at <http://hdl.handle.net/1721.1/97690>.

Laws that prohibit encryption will make companies less competitive on this indicator, not to mention they will make the Internet less safe and less free. While some politicians' public statements have portrayed encryption as something that primarily enables criminal activity, this indicator is included in the Index because we support the view that encryption is the Internet user's strongest defense against malicious hacking, identity theft, financial fraud, theft of intellectual property, and other serious crimes. Encryption is also necessary to protect the freedom of expression and physical safety of journalists, human rights defenders, political activists, and ordinary users from growing mass surveillance, including from countries that routinely imprison their citizens because of what they say online.<sup>49</sup>

---

49. See the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, on “Encryption, anonymity, and the human rights framework”, 22 May 2015, <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>. For further details on the importance of encryption, we refer the reader to the following resources: *Crypto*, by Steven Levy (2001); *Data and Goliath*, by Bruce Schneier (2015); and Global Voices' weekly *Netizen Report*.

# 5. COMPANY REPORTS

---

<b>5.1 Internet Companies</b>	33
Facebook, Inc	33
Google	35
Kakao Corp.	37
Mail.ru Group	39
Microsoft	41
Tencent	43
Twitter, Inc	45
Yahoo	47
<b>5.2 Telecommunications Companies</b>	49
América Móvil	49
AT&T	51
Axiata	54
Bharti Airtel	56
Etisalat	59
MTN	61
Orange	64
Vodafone	67

### Facebook, Inc.

[www.facebook.com](http://www.facebook.com)

NasdaqGS: FB

**Facebook, Inc.** operates social networking platforms for users globally. Lead among these is the Facebook mobile app and website that enables people to connect and share; Messenger, a mobile-to-mobile messaging application; Instagram, a mobile photo and video sharing app; and WhatsApp Messenger, a cross-platform mobile messaging application. In addition to these platforms, it also provides tools to enable developers to create mobile and web applications that enable integration of external content into Facebook's platforms. As of December 2014, it had 1.19 billion monthly active users and 890 million daily active users.

**Services evaluated:**

Facebook (social network)  
Instagram (photo and video sharing)  
WhatsApp (messaging platform)

**Industry:**

Internet Software and Services

**Domicile:** United States

**Market Cap:** USD 274,823 million\*

### OVERALL SCORE - 41%

Facebook, Inc. placed sixth out of eight Internet companies in its overall score. The company's performance across all categories suffered because its disclosure sometimes did not include Instagram. Disclosure by and about WhatsApp was markedly less and of poorer quality than disclosure pertaining to its namesake service, the Facebook social network. If the company Facebook, Inc. had been evaluated on the strength of its policies and commitments pertaining to the Facebook service alone, its total score would have been substantially higher. Facebook, Inc. acquired Instagram in 2012 and WhatsApp in 2014. The Index methodology holds a corporation responsible for the policies and practices of a new service, subsidiary, or acquisition after an initial six-month period. Given the growing use of Instagram (400 million users<sup>1</sup>) and WhatsApp (900 million users<sup>2</sup>) around the world, Facebook, Inc. should be held fully responsible for whether – and the extent to which – Instagram and WhatsApp demonstrate respect for users' freedom of expression and privacy.

### COMMITMENT - 62%

Even while losing points due to WhatsApp, Facebook Inc.'s disclosure about its commitments, and efforts to implement them, earned the company fourth place in this category, at it was more than twenty percentage points ahead of the next company, Kakao. Facebook, Inc. joined the Global Network Initiative (GNI) in 2013. Its disclosures related to human rights impact assessment (Indicator C4) were minimal; after the company completes its first round of assessment as a new member of the GNI, the company's score will likely rise in the direction of the GNI's founding companies.

Facebook Inc. has no evidence of board-level oversight for issues relating to freedom of expression and privacy, and the company's public disclosure offers no information on whether executive and management oversight has been extended to WhatsApp (C2). The company offers little in the way of public disclosure about grievance and remedy mechanisms (C6) for users who believe their freedom of expression or privacy rights were infringed in connection with the company's business.

\* S&P Capital IQ, Accessed October 16, 2015.

1. See <http://www.cnbc.com/2015/09/23/instagram-hits-400-million-users-beating-twitter.html>

2. See <http://fortune.com/2015/09/04/whatsapp-900-million-users/>

## FREEDOM OF EXPRESSION - 35%

Facebook, Inc. came sixth out of eight Internet companies on Freedom of Expression, and its score was almost half of the highest score in this category. In some cases, the company's score was dragged down by lack of disclosure and poorer-quality policies of Instagram and Whatsapp. In one case however the reverse was true: On disclosure about identity policy (F11), the Facebook service scored zero points because it can require users to verify their identity, either with government-issued identification or other forms of ID connected to offline identity. WhatsApp and Instagram earned full credit on this indicator because they do not require the same sort of ID checks.

**Transparency about requests for content restriction:** Facebook, Inc. earned high marks for clearly disclosing what types of content or activities it does not permit and how it enforces its rules (F3). However the company did much worse on disclosure about the circumstances under which it may restrict or deny users from accessing the service (F4). Among Internet companies that publish transparency reports about government requests to restrict content or access to the service (F7), Facebook's disclosure is the least comprehensive and also fails to clarify whether it includes services other than the Facebook service. It provides no data about any type of private requests – from people or entities not acting under official government auspices – to remove or restrict content (F8).

**Enforcement of terms of service:** The company provides no information about the volume and nature of content that it restricts or removes in the course of enforcing its terms of service (F9). No company in the Index received credit on this indicator. Facebook, Inc. representatives made clear to our research team that, in their opinion, this type of disclosure would be neither meaningful nor helpful to users' freedom of expression.

## PRIVACY - 36%

Facebook, Inc's privacy-related disclosures and policies lagged behind all of its peers examined in the Index – except for Tencent and Mail.ru, whom it surpassed by a large margin. Similar to the company's performance in other categories, privacy-related policies for WhatsApp and Instagram were incomplete or non-existent compared to disclosure for the Facebook service.

**Handling of user information:** Facebook, Inc. does a better job than the other U.S.-based Internet companies on disclosures about the collection of user information (P3) although it lags behind Kakao. The company's disclosure about collection of user information from third parties (P8) was especially poor, and like most companies, Facebook, Inc. ignores the “Do Not Track” standard that allows users to opt-out of certain types of web tracking.<sup>3</sup> While the Facebook service provides users with some options to control the company's sharing of their information (P5), there was insufficient evidence that WhatsApp and Instagram offer similar options. The company's disclosures about if and why it shares user information with third parties (P4) were in the middle of a group that generally needs improvement. Disclosure about retention of user information (P7) was much better for the Facebook service than for Instagram and WhatsApp, though the Facebook service still only received partial credit. Similarly, while the Facebook service earned full points for enabling users to view the information it holds about them (P6), WhatsApp and Instagram offered less to no information, respectively.

**Transparency about requests for user data:** Transparency reporting on third-party requests for user data (P11) was fairly strong for the Facebook service, but the company's disclosure provided no information as to whether Instagram and WhatsApp were included. While a company representative told our research team in private communications that the company's transparency reporting includes Instagram, that information is not available to users who lack personal connections to company staff and therefore does not meet the requirements for credit, according to the Index methodology.

**Security:** On security practices (P12) the Facebook service received a high (though not perfect) score, but there was little disclosure for the other services. The company received no credit on encryption of private user content (P13) because users of the Facebook service and Instagram cannot encrypt their private messages. Also, while WhatsApp states that, “WhatsApp communication between your phone and our server is encrypted,” the service provides insufficient detail to determine whether user content is encrypted in a way that the company has no access. Although the score for this indicator is based on company disclosure, it is worth noting that Open Whisper Systems, which has partnered with WhatsApp, states, “The WhatsApp Android client does not yet support encrypted messaging for group chat or media messages,”<sup>4</sup> suggesting that encryption is not available throughout the service. Likewise, we found no information about encryption on other platforms such as iOS and Windows Phone. Finally, while the Facebook service has taken steps to educate users about security threats (P14), Instagram's weaker disclosure and WhatsApp's lack of disclosure dragged down the company's score on this indicator.

3. See <http://donottrack.us/>.

4. See <https://whispersystems.org/blog/whatsapp/>

# Google, Inc.

www.google.com

NasdaqGS: GOOGL

**Google, Inc.** (now a subsidiary of Alphabet Inc.) is a major global technology company that develops a range of products and services that facilitate discovery and management of information. Alongside its significant suite of consumer applications and devices, Google also provides advertising services, which account for a significant majority of its revenues. It primarily delivers services via the Internet, and it has also expanded into consumer hardware products.

## Services evaluated:

Google Search (Internet search engine)  
Gmail (email platform)  
YouTube (video sharing platform)

## Industry:

Internet Software and Services

**Domicile:** United States

**Market Cap:** USD 466,718 million\*

## OVERALL SCORE - 65%

Google, a founding member of the Global Network Initiative (GNI), earned the highest overall score in the Index. However there is much room for improvement. While aspects of U.S. law and the company's business model would need to change in order for Google to achieve a perfect score, the company's score could improve substantially even if its business model and the legal and regulatory environment in the United States were to remain unchanged. If the company were simply to match the top-scoring company for each indicator in the Index, its overall score would rise by nearly 10 percentage points.

## COMMITMENT - 78%

Google came in third place on disclosed commitments and mechanisms to implement them, behind Yahoo and Microsoft, whose disclosures were more clearly articulated and thorough. Our researchers found no evidence of board-level oversight of the company's practices that affect users' freedom of expression and privacy (Indicator C2). On human rights impact assessments (C4) the company ties with Microsoft but is overtaken by Yahoo. While Google's grievance and remedy mechanisms are somewhat better than those of other U.S.-based Internet companies, Google falls behind the Internet company Kakao and the telecommunications companies Bharti Airtel, América Móvil, and Vodafone on articulating specific ways that stakeholders can communicate grievances to the company and see those grievances addressed (C6).

## FREEDOM OF EXPRESSION - 68%

Google substantially outperformed all other companies in the Index on Freedom of Expression. The company was particularly strong in disclosing its process for responding to third-party requests to restrict content or restrict users' access to the service (F6). "Transparency reporting" about government requests was also strong across the board (F7). Google was second only to Twitter in its process for notifying users about restrictions (F5) although the highest score for that indicator was only 50 percent.

\* S&P Capital IQ, Accessed October 16, 2015.

**Private requests for content restriction:** The company could better disclose information about private requests to restrict content or access to services. While the company provides data for Google Search on requests related to copyright infringement and related to the “Right to be forgotten” ruling in Europe, it provides no data about private requests to restrict content on YouTube (F8).

**Enforcement of terms of service:** As with all companies evaluated in the Index, users and the public generally have no insight into the volume and nature of actions that Google initiates to enforce its own terms of service (F9).

## PRIVACY - 57%

On disclosures related to privacy, Google finds itself at the top of a cluster of companies whose performance nonetheless remains unsatisfactory – despite some laudable efforts in particular areas such as transparency about government requests for user data.

**Handling of user information:** Along with its peers, Google generally suffered from lack of clarity and specificity in its disclosures related to the handling of user information (see Section 4.3) It performed substantially worse than its peers on disclosures about whether it collects user information *from* third parties (P8), and there is no evidence that it respects the “Do Not Track” standard that allows users to opt-out of certain types of web tracking.<sup>1</sup> Its disclosure about the sharing of user information *with* third parties (P4) was much weaker than all other Internet companies except Mail.ru, (although no company scored higher than 51 percent on this indicator). It was surpassed by Twitter and Microsoft in disclosures about retention of user information (P7).

**Transparency about requests for user data:** On “transparency reporting” about third-party requests for user data (P11), Google placed second behind Twitter, with Yahoo close on its heels, for the range of its disclosure. Notably, while Google does notify users about requests for user data made through subpoenas in civil court cases (P10) its transparency report does not include data about requests from civil subpoenas that involve private parties. A concrete example is when Chevron issued subpoenas to several email services, including Gmail, in 2012 for information related to the accounts of several people involved in a lawsuit against the oil company. Google notified the users whose information had been requested about the subpoena (which it subsequently challenged in court).<sup>2</sup> However data about that request, and other such requests made by private entities involved with litigation or otherwise, are not included in Google’s transparency report.

**Security:** Google is exemplary in its approach to educating users about security threats (P14). Its score on security standards (P12) was relatively high but could be improved with some basic disclosure about whether it regularly conducts security audits (information that Vodafone and AT&T have disclosed). It also lost points on that same indicator for vague and out-of-date disclosures about what systems it has in place to limit and monitor employee access to user information.

**Encryption:** On disclosure about whether the company enables users to encrypt their own content (P13), Google received partial credit. The “safer email” section of Google’s Transparency Report discusses PGP encryption (which users need to set up themselves, independently of Gmail’s features, using third-party tools) as an option for at-risk users. This disclosure acknowledges that users can encrypt their Gmail content, however, companies can only receive full credit on this indicator if they provide such encryption by default. Notably, the company’s page on “End-to-End Encryption” states that it is developing a new feature that would allow users to encrypt messages with a built-in option. Once such a feature is available to all users, the company could earn a higher score.

1. See <http://donottrack.us/>.

2. Declan McCullagh, “Chevron targets Google, Yahoo, Microsoft e-mail accounts,” *CNet*, October 11, 2012, <http://www.cnet.com/news/chevron-targets-google-yahoo-microsoft-e-mail-accounts/>.

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

#### Services evaluated:

Daum Search (online search portal)  
Daum Mail (email platform)  
KakaoTalk (messaging platform)

#### Industry:

Internet Software and Services

**Domicile:** South Korea

**Market Cap:** USD 6,105 million\*

## OVERALL SCORE - 47%

Kakao placed fifth among Internet companies, behind Twitter and ahead of Facebook. The company changed its name in September 2015 to “Kakao” from “Daum Kakao,” the name it had used since the merger of two companies Daum and Kakao in 2014.<sup>1</sup> While South Korea’s Internet is rated only “partly free” by Freedom House’s 2015 “Freedom on the Net” index,<sup>2</sup> the country has a strong civil society, lively press, and competitive political system, all of which have contributed to the emergence of public demands for greater transparency by companies and government, particularly in relation to surveillance.<sup>3</sup> Kakao’s commitments and disclosures related to freedom of expression and privacy are significantly stronger than any other non-Western company examined in the Index. Its privacy practices also reflect South Korea’s strong legal framework for data protection. Notably, Kakao earned leading scores on eight indicators in the Index, with five of those surpassing any other company evaluated.

## COMMITMENT - 39%

Kakao placed fifth among Internet companies for its disclosure of commitments and evidence of accompanying measures to implement those commitments. It surpassed Twitter by four percentage points in this category but trailed the other four U.S.-based Internet companies (all of which are members of the Global Network Initiative) by a substantial margin. Kakao earned at least some points on every indicator in this category.

**Balance of commitments:** Kakao’s commitments and related implementation tended to be stronger for privacy than for freedom of expression. For example, we found publicly disclosed evidence of executive and management oversight (Indicator C2) on user privacy issues, but no evidence of similar oversight for freedom of expression. We found public disclosure on training and internal whistleblower mechanisms (C3) for privacy but not freedom of expression. Kakao operates within a legal context that involves restrictions on freedom of expression that have been criticized domestically and internationally as being counter to international human rights norms.<sup>4</sup> Nonetheless, the company faces no legal barriers to commit to respect users’ freedom of expression at the same level of its commitments to privacy.

**Engagement:** Kakao is an active member of industry organizations that engage with stakeholders, and the company earned credit for this stakeholder engagement (C5).

\* S&P Capital IQ, Accessed October 16, 2015.

1. See <http://www.zdnet.com/article/kakao-commences-leadership-change-with-young-ceo-on-top/>.
2. South Korea, *Freedom on the Net 2015*, Freedom House, <https://freedomhouse.org/report/freedom-net/2015/south-korea>.
3. See <http://transparency.kr/?ckattempt=1> and <http://www.nytimes.com/2015/04/03/opinion/south-koreas-invasion-of-privacy.html>.
4. South Korea, *Freedom on the Net 2015*, Freedom House, <https://freedomhouse.org/report/freedom-net/2015/south-korea>.

**Remedy:** On grievance and remedy processes (C6) Kakao received a higher score than any other Internet company evaluated in the Index. This is largely due to requirements under South Korea’s Act on Promotion of Information and Communications Network Utilization and Information Protection.<sup>5</sup> On freedom of expression, Kakao goes beyond the law by providing users with an appeals mechanism when content is removed in compliance with requests made under anti-defamation law.

## FREEDOM OF EXPRESSION - 59%

Kakao placed second behind Google among Internet companies – and in the Index overall – on Freedom of Expression. It earned leading scores on four of the ten indicators in this category, with two of those surpassing all other companies evaluated. Most notably, Kakao earned the highest score of the entire Index on indicator F2, which examines whether the company provides notice and record of changes to its terms of service – an indicator on which most companies fared poorly. In fact, Kakao received full scores on this indicator for Daum Search and Mail, while KakaoTalk’s weaker disclosure brought down the company’s overall score to 83 percent. The company discloses in great detail its reasons for content restriction (F3) and account or service restriction (F4), and it provides examples to help users understand these company policies.

**Transparency about requests for content restriction:** Kakao publishes a transparency report that includes more information about requests for content restriction than many of its Internet peers. Furthermore, its transparency report contains more data about private requests to restrict content (F8) than any other company in the Index, although it still received fewer than half of the total possible points for that indicator. However, there are limits to how much detail the company can disclose. Company representatives told our research team that the company is legally prohibited from publishing copies of original documents that request content restriction.

## PRIVACY - 42%

Kakao placed fifth among Internet companies on Privacy, ahead of Facebook and behind Twitter. It earned leading scores on four of the 14 indicators in this category, with three of those higher than any other company evaluated.

**Handling of user information:** Notably, the company’s disclosure about collection of user information (P3) greatly surpassed any other company in the Index. Disclosure about the sharing of user information (P4) tied with Yahoo, the other top performer on this indicator. On some other indicators, Kakao lagged behind its peers. The company does not offer users any meaningful options to control what user information the company collects or shares (P5), and similarly, it offers users no means to access the information the company holds about them (P6). Disclosure about retention of user information (P7) was minimal for Daum Search and Mail, though much better for KakaoTalk. The company discloses nothing about collection of user information from third parties (P8) although in feedback to our research team, company representatives pointed out that companies are required by law to disclose such a practice if they engage in it.

**Transparency about requests for user data:** Kakao discloses a considerable amount of information about its process for responding to third-party requests for user information (P9). It discloses as much information about the volume and nature of third-party requests for user data (P11) as AT&T and Microsoft, though less than Twitter, Google, and Yahoo. However, the company is constrained by law in terms of the types of notification it can provide to users about government requests for user information (P10).

**Security:** KakaoTalk’s “secret chat” function offers full encryption of the contents of user conversations, earning Kakao first place in the entire Index on encryption of users’ private content (P13). Its disclosure about security practices (P12) was highest among all Internet companies examined. While Kakao’s performance on these two security-related indicators was superior, the company itself does not provide any user education about security threats (P14). Instead, company representatives indicated that a government website makes such information available to Korean users. To receive credit on this indicator, companies must provide such disclosure on their own sites.

5. See Greenleaf, Graham and Park, Whon-il, Korea’s New Act: Asia’s Toughest Data Privacy Law (July 19, 2012). Privacy Laws & Business International Report, Issue 117, 1-6, June 2012; UNSW Law Research Paper No. 2012-28. <http://ssrn.com/abstract=2120983>; and <http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&vSct=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#0000> (Korean).



# Mail.ru Group Limited

<http://corp.mail.ru>

LSE: MAIL

**Mail.ru Group Limited**, together with its subsidiaries, provides online communication products and entertainment services in Russia and internationally. The company operates through five segments: Email, Portal and IM; Social Networks; Online Games; Vkontakte (VK); and Search, E-Commerce and Other Services. These segments deliver social platforms or services that enable online communications and sharing, offer games or entertainment, provide advertising services, support e-commerce and in application purchases, and deliver search services.

## Services evaluated:

Vkontakte (social network)  
Mail.ru (email platform)  
Mail.ru Agent (messaging platform)

## Industry:

Internet Software and Services

**Domicile:** Russia

**Market Cap:** USD 3,996 million\*

## OVERALL SCORE - 13%

Mail.ru had the lowest score of all companies in the Index. The Russian Internet was rated “not free” by Freedom House’s 2015 “Freedom on the Net” index.<sup>1</sup> Internet companies operating in Russia are governed by laws that give authorities broad powers to create “blacklists,” hold companies responsible for policing user content, and require companies to block and remove content.<sup>2</sup> A recent study indicates relatively broad support for censorship in Russia.<sup>3</sup> Russian law also requires companies to implement a mass surveillance system called SORM, which enables security services to access all user data.<sup>4</sup> These factors contribute to an environment in which Russian companies face little incentive to make public commitments to respect users’ freedom of expression and privacy. Nonetheless, there is room within Russian law for Mail.ru to make efforts that could result in stronger performance on many of the Index indicators.

## COMMITMENT - 2%

Mail.ru scored lowest among Internet companies on Commitment, and it was second to last of all companies in the Index. In this category, it only received some credit for grievance and remedy mechanisms (Indicator C6) because the company’s mail and chat services, but not the social network Vkontakte, have a provision in their user agreement that users who believe their “rights and interests are infringed by the actions of Mail.Ru shall be entitled to lodge a claim.” Russian law does not specifically prevent Mail.ru from strengthening its policy commitments and grievance and remedy mechanisms, in addition to other efforts such as oversight (C2), training, (C3), and impact assessment (C4) outlined in this category.

\* S&P Capital IQ, Accessed October 16, 2015.

1. See <https://freedomhouse.org/report/freedom-net/2015/russia>.

2. Olga Razumovskaya, “Russian Parliament Approves New Law Restricting Internet,” *The Wall Street Journal*, April 29, 2014, <http://www.wsj.com/articles/SB1000142405270230416360457953146021555456>.

3. Eric Nisbet with the Center for Global Communication Studies and the Russian Public Opinion Research Center, *Benchmarking Public Demand: Russia’s Appetite for Internet Control*, Center for Global Communication Studies at the University of Pennsylvania, February 2015, <http://www.global.asc.upenn.edu/publications/benchmarking-public-demand-russias-appetite-for-internet-control/>.

4. See <http://www.zakonrf.info/koap/13.31/> and James Andrew Lewis, Reference Note on Russian Communications Surveillance, Center for Strategic and International Studies, April 18, 2014 <https://csis.org/publication/reference-note-russian-communications-surveillance>.

## FREEDOM OF EXPRESSION - 23%

Mail.ru placed second to last among Internet companies on Freedom of Expression. Its score in this category surpassed that of Tencent because the company does not subject mail and chat users to identity checks (F11). Beyond having publicly available terms of service (F1), the company's only other disclosures for this category related to informing users about reasons why it may restrict content and access to the service (F3 and F4).

**Transparency about requests to restrict content:** Russian law does not specifically prevent companies from being more transparent about their processes to handle third-party requests and terms of service enforcement. While Russian law has not been tested in this regard, it does not appear to prevent the company from publishing at least some data related to some types of restriction requests it receives. However legal experts we consulted point to Russia's rapidly evolving regulatory landscape, which is trending towards stronger restrictions, thus dis-incentivizing companies from testing legal boundaries in the direction of respecting users' freedom of expression.

## PRIVACY - 11%

On Privacy, Mail.ru scored fewer points than any other company in the entire Index.

**Handling of user information:** Mail.ru does not offer publicly available privacy policies for two of the three services examined (Mail and chat). The company's disclosures about what user information it collects (P3) and shares (P4) are notably weaker than the Chinese company, Tencent. Based on our understanding of Russian law, it should be possible for Mail.ru to disclose more about how and why the company collects, shares, and retains user information. It should also be possible for the company to disclose to users what information about them it holds.

**Transparency about requests for user data:** Russian law, which requires all user data to be shared with authorities, is also interpreted to prevent companies from sharing information related to government requests (P9, P10, P11). Experts and resources we consulted indicate that the line between government and private requests is generally blurry, creating strong disincentives for companies to disclose any type of requests for user data.

**Security:** The company does provide some information about security standards (P12); notably, it offers "two step authentication" across two of the three services examined. It also offers some user education about cyber threats (P14).

# Microsoft Corp.

www.microsoft.com

NasdaqGS: MSFT

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

## Services evaluated:

Bing (search engine)  
Outlook.com (email platform)  
Skype (chat and Internet calling)

## Industry:

Software

**Domicile:** United States

**Market Cap:** USD 379,984 million\*

## OVERALL SCORE - 56%

Microsoft, a founding member of the Global Network Initiative, placed third in the overall Index as well as among Internet companies. While it performed strongly on the Commitment category, it scored under 50 percent of total possible points on the Freedom of Expression category, demonstrating room for improvement. On October 14, 2015 – two weeks after the final cutoff date for incorporating any new information into the Index – the company unveiled a new Transparency Hub that contained new disclosures, most notably some with strong relevance to the Freedom of Expression category.<sup>1</sup> We look forward to including that information – or even newer disclosures – in future iterations of the Index.

## COMMITMENT - 82%

Microsoft earned top marks in the Index overall on its disclosed commitments to users' freedom of expression and privacy and accompanying measures to implement those commitments. It received full marks on four of the six indicators in this category, including Indicator C2, which focused on governance and management oversight. Unlike Google and Yahoo, Microsoft discloses that its board of directors exercises oversight on human rights issues including freedom of expression and privacy. The company's high score for human rights impact assessment (C4) was exceeded only by Yahoo.

**Remedy:** Within the Commitment category, Microsoft's greatest area of improvement focuses on grievance and remedy mechanisms (C6). While the company offers support websites where users can ask questions and submit complaints, these websites do not explicitly mention that such channels are meant to handle human rights grievances in relation to freedom of expression and privacy. Moreover, the company does not clarify its process for responding to such complaints or report on how it has handled them historically. In addition, some dispute resolution mechanisms are only available to U.S. users.

\* S&P Capital IQ, Accessed October 16, 2015.

1. See <http://blogs.microsoft.com/on-the-issues/2015/10/14/new-transparency-hub-debuts-with-latest-reports/>.

## FREEDOM OF EXPRESSION - 46%

Freedom of Expression was Microsoft's weakest area, based on information collected through the end of September 2015. As noted above, the company's new Transparency Hub, unveiled in mid-October, came too late for its disclosures to be incorporated into the Index dataset. The company placed fifth in this category behind Google, Kakao, Twitter, and Yahoo.

**User notification about content restriction:** On indicator F5, which examined companies' commitments to notify users when content is restricted, Microsoft's score was substantially lower than several peers including Twitter, Google, Kakao and Facebook. In communications with our research team about this indicator, a company representative emphasized the need for "balance" between freedom of speech and "safety of end users and lawful operations of our services." Specifically, the company cited the need to consider user privacy, victim safety, and government gag orders when deciding whether to notify users about content or account restriction.

**Enforcement of terms of service:** Like other companies in the Index, Microsoft discloses no information about the volume and nature of content or accounts that it restricts in the course of enforcing its terms of service (F9). In feedback to our researchers, a company representative cited user privacy as one reason for not disclosing such information, along with the fact that the company has prioritized transparency about other types of data, such as government requests. However the representative indicated that the company is open to a discussion of "ways to include information about terms of service enforcement that respect customer privacy."

## PRIVACY - 53%

Microsoft came in second place on privacy-related disclosures, an area in which all companies have much room for improvement.

**Handling of user information:** The company's disclosure about collection of user information (P3) was on par with many peers, though not the strongest of all companies evaluated. Disclosure about the sharing of user information (P4) outperformed Google but was surpassed by Kakao, Yahoo, Facebook and Tencent. However, even the highest-scoring companies still fell seriously short of what users have a right to know. Microsoft could do more to help users access the information about them the company holds (P6). It could also provide more information about retention of user information (P7) and collection of user information from third parties (P8). Like many companies in the Index, Microsoft does not respect the "Do Not Track" standard (P8) that allows users to opt-out of certain types of web tracking.<sup>2</sup>

**Transparency about requests for user data:** Microsoft tied with Google for providing information about its process for responding to third-party requests for user data (P9). (See Section 4.3 as well as Section 1 for discussion of different types of third-party requests.) Microsoft was surpassed only by Yahoo in its commitment to notify users about third-party requests for user data (P10). The company's "transparency reporting" about third-party requests for user data (P11) was strong, though less thorough than Twitter, Google and Yahoo.

**Security:** Microsoft disclosed substantially less information about security standards (P12) than several of its peers. User education about security threats (P14) was exemplary for Bing and Outlook but weaker for Skype. Microsoft does not presently offer ways for users to encrypt the content of their private communications or encourage the use of third-party encryption solutions (P13). However in a statement to our research team, a company representative indicated that this might change, stating, "Microsoft appreciates the importance of this issue and is exploring ways to provide customers with the option to encrypt their content such as their emails in Outlook.com."

2. See <http://donottrack.us/>.

# Tencent Holdings Limited

www.tencent.com

SEHK: 700

**Tencent Holdings Limited** provides a broad range of Internet and mobile value-added services (VAS), online advertising services, and eCommerce transactions services to users in China, the United States, Europe, and elsewhere around the world. It is one of the largest Internet companies globally.

## Services evaluated:

QZone (social network)  
QQ (instant messaging)  
WeChat (mobile messaging/calling)

## Industry:

Internet Software and Services

**Domicile:** China

**Market Cap:** USD 176,038 million\*

## OVERALL SCORE - 16%

Tencent's score was second lowest among Internet companies examined, and it ties for third lowest in the Index overall. Tencent's performance in the Index was heavily affected by the laws, regulations, and policies of its home country government. China is rated "Not Free" in Freedom House's 2015 "Freedom on the Net" Index.<sup>1</sup> The country holds Internet companies strictly liable for users' activities.<sup>2</sup> Companies are required to monitor and police user behavior and work closely with police and national security authorities, largely without judicial oversight or avenues for legal remedy.<sup>3</sup> State secrets laws prevent companies from being transparent about the nature and volume of government requests to restrict content or hand over user data, let alone provide detail about company policies and practices for handling such requests.

Even in the current legal and regulatory environment, Tencent can take concrete steps to improve its commitment to and respect for users' rights.

## COMMITMENT - 8%

Tencent scored second to last among Internet companies, and fourth from last overall in the Index, on commitments to users' freedom of expression and privacy. It received some credit on policy and leadership commitment (Indicator C1) due to statements regarding company commitments to user privacy. However, the company lacks similar commitments in support of freedom of expression. The company also received a few points for grievance and remedy mechanisms (C6) because it offers a contact point to report infringement of rights including "civil rights." But information about this contact point is only found in the terms of service directed at international users residing outside of mainland China – and not in the version governing users in the home market.

The company should offer the same level of respect for mainland Chinese users' rights as it offers to its international users.

\* S&P Capital IQ, Accessed October 16, 2015.

1. China, *Freedom on the Net 2015*, Freedom House, <https://freedomhouse.org/report/freedom-net/2015/china>.

2. WILMAP: China, The Center for Internet and Society at Stanford Law School, <http://cyberlaw.stanford.edu/page/wilmap-china>.

3. Eva Dou, August 6, 2015, China to Embed Internet Police in Tech Firms, *Wall Street Journal*, <http://www.wsj.com/articles/china-to-embed-internet-police-in-tech-firms-1438755985>.

## FREEDOM OF EXPRESSION - 19%

Tencent was the lowest-scoring Internet company on Freedom of Expression, and the second lowest-scoring company on this category in the Index overall. The company received points on three indicators in this category: the availability of terms of service (F1), reasons for content restriction (F3), and reasons for account or service restriction (F4).

**Transparency about requests for content restriction and enforcement of terms of service:** The company does not publicly commit to notify users when it restricts access to their accounts, removes content posted by users, or blocks messages transmitted by users (F5). However, our researchers did find anecdotal evidence that users receive notifications with the message: “This content has been reported on by many users; you cannot view the relevant content.” The company’s public commitments or policy disclosures do not support such anecdotal evidence; consequently the company received no score on this indicator.

While state secrets laws make it unrealistic to expect greater company transparency about Chinese government requests, the company could make efforts to disclose requests made by other governments in markets where it serves significant numbers of users. In all markets, it would be reasonable for users to expect greater transparency about private requests and terms of service enforcement, to the maximum extent possible under the law.

## PRIVACY - 17%

Tencent was the second-lowest scoring Internet company on privacy-related disclosures, although it placed ahead of three telecommunications companies. Tencent does have a publicly accessible and reasonably clear company-wide privacy policy (P1). When it comes to providing notice and record of changes to its privacy policies (P2) Tencent’s disclosures are similar or even greater than several companies whose overall scores in the Index were much higher.

**Handling of user information:** Tencent received scores on three other indicators in the Privacy category. On disclosures about collection of user information (P3), it received the same overall score as Google, Microsoft, Twitter, and Vodafone and was surpassed only by Kakao and Facebook. On disclosures about the sharing of user information with third parties (P4), its score was the same as AT&T and Facebook, surpassed only by Kakao and Yahoo. However, the company should make efforts to enable all users – in mainland China as well as externally – to view the information that the company holds about them (P6).

**Transparency about requests for user data:** The company discloses no information related to its policies and practices for handling third-party requests for user data.

**Security:** Tencent also received some credit on indicator P14, which focuses on user education about cyber threats. The company’s messaging service QQ has an online “security center” with tips about account protection that include cartoons and graphics. The company should make efforts to improve security practices and provide such materials for all of its services.

# Twitter, Inc.

<http://twitter.com/>

NYSE: TWTR

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

## Services evaluated:

Twitter (micro-blogging platform)  
Vine (video creation and sharing)

## Industry:

Internet Software and Services

**Domicile:** United States

**Market Cap:** USD 21,067 million\*

## OVERALL SCORE - 50%

Among Internet companies in the Index, Twitter came in fourth overall behind Google, Yahoo, and Microsoft. Twitter executives have long trumpeted the company's role as a tool for individual empowerment. The company declares that its mission is "To give everyone the power to create and share ideas and information instantly, without barriers."<sup>1</sup> On October 5, 2015, Twitter's co-founder and newly appointed CEO Jack Dorsey declared in a tweet: "Twitter stands for freedom of expression. We stand for speaking truth to power. And we stand for empowering dialogue."<sup>2</sup> Our research indicates that Twitter is indeed a leader in freedom of expression and very competitive on its concrete policies and practices that affect users' privacy. However when it comes to demonstrating governance and oversight, internal accountability, and institutionalization of its commitments at the corporate level, the company falls short of its peers, bringing down its overall score.

## COMMITMENT - 35%

On publicly articulated commitments and disclosed efforts to implement those commitments, Twitter came in sixth, behind Kakao and substantially behind the other U.S.-based Internet companies. Company commitments and executive statements related to freedom of expression and privacy are scattered around the company website, blog posts, and Twitter feeds of individual executives and departments. This makes it difficult for a specialized researcher, let alone a general user, to form a clear picture of executive commitment and responsibility without help from company employees who can point to the location of specific blog posts and tweets.

Throughout Twitter's disclosure, there is no evidence of board oversight on matters related to freedom of expression and privacy (Indicator C2). In contrast to many of its peers, Twitter publishes no information about whether it conducts employee training on freedom of expression or privacy (C3). Information about its internal whistleblower program appears to focus on user privacy but not freedom of expression (C3). The company does not disclose whether it conducts human rights impact assessments (C4). While it engages with stakeholders (C5), it does not participate in a multi-stakeholder organization in which civil society, responsible investors, and academics can hold the company accountable for its practices. Twitter's mechanisms for grievance and remedy (C6) do not stand out among the company's U.S.-based peers.

\* S&P Capital IQ, Accessed October 16, 2015.

1. See <https://about.twitter.com/company>.
2. See <https://twitter.com/jack/status/651003891153108997>.

## FREEDOM OF EXPRESSION - 58%

Twitter is a relatively strong performer on Freedom of Expression, ranking third behind Google and closely behind number two, Kakao. Twitter's terms of service are exemplary in their clarity and accessibility (F1). The company could further improve its performance if it takes steps to bring the policies of Vine, its video service, into closer alignment with the core Twitter service. In some cases, the company's public disclosures did not clarify whether they included Vine. Because company scores in this category were calculated as an average of the services evaluated, a very high score for the core Twitter service was sometimes diluted by a low score for Vine.

**Transparency about requests for content restriction:** The core Twitter service is a leader on transparency reporting related to content removal and restriction. For example, Twitter forwards content removal requests to ChillingEffects.org, which publishes these requests as part of an online repository of specific requests for content restriction that Internet services receive. By doing so, Twitter increases the broader public's ability to hold both Twitter and the senders of content restriction requests to account.

On disclosure of data about government requests to restrict content (F7), the core Twitter service scored higher than any other company except Google. While a company representative told our research team in private communications that the company's transparency report on government requests for content restriction includes Vine, that information is not available to users who lack personal connections to company staff. Such information does not meet the Index methodology's requirements for consideration, and consequently, Vine received no credit on that indicator. Some other companies in the Index have done a better job of clarifying what their transparency reports do or do not include. Twitter's Index score could rise significantly in the future if the company offers similar clarity.

## PRIVACY - 51%

On privacy-related disclosures, Twitter clusters closely with the top four Internet companies, though much room for improvement remains.

**Handling of user information:** Similar to its peers, Twitter's disclosures related to the handling of user information suffered from lack of clarity and organization (see Section 4.3). For example, its disclosure of what information Twitter shares with third parties (P4) failed to clearly define or explain the use of terms such as "your information" and "private personal information."

As discussed in the Freedom of Expression category above, an easy way for Twitter to boost its Index score on privacy would be to bring its policies and disclosures for Vine into alignment with those for the core Twitter service. If not for Vine, Twitter would have been tied in first place with Google for enabling users to access their own information (P6).

More positively, Twitter was a leader in some regards: It earned the highest score in the Index on disclosure of how long it retains user information (P7). On disclosure about the collection of user information from third parties using web-tracking technologies (P8), Twitter is the clear leader. Its core Twitter service is the only service in the Index to support the "Do Not Track" standard that allows users to opt-out of certain types of web tracking.<sup>3</sup>

**Transparency about requests for user data:** Twitter performed better than any other company in the Index on privacy-related "transparency reporting." It publishes more comprehensive data than other companies about third-party requests for user information (P11). Twitter was very competitive with its peers on disclosure about its process for responding to third-party requests for user information (P9), and on notifying users about third-party requests for user information (P10).

**Security:** Vine's score was markedly worse than the core Twitter service on security standards (P12), and on practices to inform and educate users about cyber threats (P14). The company lost points for failing to encrypt users' private communications (P13) – in the case of Twitter that means the service's "direct message" function.

3. See <http://donottrack.us/>.



# Yahoo! Inc.

www.yahoo.com

NasdaqGS: YHOO

**Yahoo! Inc.** provides a broad range of communication, sharing, and information and content services. Its services include the search platform Yahoo Search, communication and collaboration tools including Yahoo Mail, Yahoo Messenger, and Yahoo Groups, digital content through Yahoo.com, Yahoo Sports, and Yahoo Finance, advertising services, and multiple other services and properties.

## Services evaluated:

Yahoo Mail (email platform)  
Flickr (photo management and sharing)  
Tumblr (blogging platform)

## Industry:

Internet Software and Services

**Domicile:** United States

**Market Cap:** USD 31,414 million\*

## OVERALL SCORE - 58%

A founding member of the Global Network Initiative (GNI), Yahoo received the second highest overall score in the Index, behind Google and slightly ahead of Microsoft. The company's disclosures related to freedom of expression and privacy are overseen by the Yahoo Business and Human Rights Program, established in 2008 to help integrate human rights-related decision-making into the company's business operations.<sup>1</sup>

## COMMITMENT - 80%

Yahoo placed second, behind Microsoft and ahead of Google, on disclosed commitments to respect users' freedom of expression and privacy rights and measures to implement those commitments. It received the highest score for human rights impact assessments (Indicator C4). On Indicator C2, which examined governance and management oversight, the company lost points due to lack of board-level oversight. A shareholder resolution calling for the creation of a board committee that would exercise formal oversight over human rights issues, including freedom of expression and privacy, was opposed by the board, on the grounds that such a committee is "not necessary or advisable and would involve making regular BHRP update to a subset of the board, rather than to the full Board, as is Yahoo's current practice."<sup>2</sup> Like all of its peers, the company has much room for improvement on grievance and remedy mechanisms (C6).

## FREEDOM OF EXPRESSION - 53%

Yahoo placed fourth among Internet companies on Freedom of Expression, behind Google, Kakao, and Twitter.

\* S&P Capital IQ, Accessed October 16, 2015.

1. Yahoo Business and Human Rights Program, <http://yahoobhrp.tumblr.com/post/75544734087/yahoo-business-human-rights-program-yahoo>.

2. Proposal 6 – Shareholder Proposal, Schedule 14(a) Proxy Statement submitted to the United States Securities Commission by Yahoo! Inc., 2014, [https://www.sec.gov/Archives/edgar/data/1011006/000119312514172132/d710905ddef14a.htm#toc710905\\_20](https://www.sec.gov/Archives/edgar/data/1011006/000119312514172132/d710905ddef14a.htm#toc710905_20).

**User notification about content restriction:** Yahoo’s commitment to notify users when it restricts content or accounts (F5) was weaker than a number of its peers. While publicly available company policies mentioned user notification related to copyright infringement, we found no publicly available information about notification for other reasons, such as enforcement of terms of service.

**Transparency about requests for content restriction:** Disclosure about the company’s process for responding to third-party requests (F6) was much weaker for Tumblr than for other Yahoo services, thus bringing down the company’s overall score on that indicator. In contrast, disclosure about private requests (F8) was stronger for Tumblr than almost any other service evaluated in the Index, but was minimal for Flickr. This caused the company’s overall score to be lower than Kakao and Google. Transparency about government requests to restrict content (F7) was approximately on par with Kakao but far behind Google.

## PRIVACY - 52%

Yahoo placed third among Internet companies on Privacy, just ahead of Twitter and slightly behind Microsoft.

**Handling of user information:** Of special note is Tumblr’s approach to posting changes to their privacy policy (P2) through the GitHub versioning system – this is a novel and interesting approach to document changes. Yahoo tied with Kakao for highest score on disclosures about sharing of user information (P4) although at 51 percent of the total possible score, much room remains for improvement. On disclosures about what user information the company collects (P3), Yahoo scored 7-14 percentage points behind several of its peers and 27 percentage points behind this indicator’s leader, Kakao. Yahoo provides fewer options for users to control the collection and sharing of information (P5) than many of its peers.

Yahoo falls short of Google and Facebook in enabling users to access to their own information (P6). Its disclosure about retention of user information (P7) falls well short of Twitter, the Index leader for that particular indicator. Like many of its peers, Yahoo has much room for improvement in disclosures about what user information it collects from third parties (P8). While it is encouraging to see that Yahoo supports the “Do Not Track” standard for the Firefox browser, companies can only receive credit in this Index for supporting the standard universally.<sup>3</sup>

**Transparency about requests for user data:** When examining the company’s transparency about requests for user data, Yahoo’s performance was strong but not in the lead. In the overall Index, it came in fourth behind Google, Microsoft, and AT&T in transparency about its process for responding to third-party requests for user data (P9). However it is notable that on P9, Tumblr was the only service of any company whose disclosure clearly states that the company does not entertain requests without valid subpoena, search warrant, or other government order. Yahoo leads the Index in notifying users about third-party requests for user data (P10), thanks particularly to the strength of Tumblr’s disclosure. In reporting information about third-party requests for user data (P11), Yahoo placed third in the Index overall behind Twitter and just one percentage point behind Google.

**Security:** Yahoo’s disclosures about security practices (P12) were dragged down by weaker disclosure from Tumblr. Similarly, Yahoo Mail and Flickr were exemplary at user education about potential threats (P14), but Tumblr, less so. The company provides no options for encryption of user content (P13), which is especially important for email. Even though the company has unveiled plans to implement PGP encryption, it hasn’t rolled this out as a built-in feature to all Yahoo users yet.<sup>4</sup>

3. See <http://donottrack.us/>.

4. See <http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption>.

## 5.2 Telecommunications Company Reports

### América Móvil, S.A.B. de C.V.

www.americamovil.com

BMV: AMX L

**América Móvil, S.A.B. de C.V.** provides telecommunications services in Mexico and internationally, including 18 countries in the Americas and seven in Europe. It offers mobile and fixed voice and data services for retail and business customers. It operates under several brands and maintains a position as one of the largest operators globally, reporting more than 289 million mobile customers, 22.5 million fixed broadband accesses, and more than 21 million television subscribers.

**Operating company evaluated:**  
Telcel (Mexico)

**Industry:**  
Telecommunication Services

**Service evaluated:** Mobile

**Domicile:** Mexico

**Market Cap:** USD 57,955 million\*

### OVERALL SCORE - 22%

América Móvil's overall Index score puts it in fourth place among telecommunications companies in the Index. Mexico was rated "Partly Free" in Freedom House's 2015 "Freedom on the Net" index.<sup>1</sup> The country's legal and regulatory environment may prevent a perfect score on all indicators in the Index; however, this is a challenge for all of the telecommunications operators in the Index, considering that operators are always subject to the country's license, rules, and regulations. This research found no explicit legal or regulatory impediments on most of the indicators.

Considering the scale of América Móvil's operations – it is one of the top five mobile telecommunications providers in the world<sup>2</sup> – its low score on commitments related to freedom of expression and privacy rights represents a considerable gap and a concern to hundreds of millions of users across multiple markets. Commitments at the corporate level would represent a strong step toward improving the company's performance and would present an ideal point of dialogue for stakeholders and company representatives. Furthermore, it is fair to expect the company to disclose information about how it handles third-party requests and to introduce a transparency report that provides the maximum amount of information as permitted by law.

### COMMITMENT - 11%

On Commitment, América Móvil's placed sixth out of eight telecommunications companies in the Index. Based on our research, the regulatory and legal context in which the company operates does not appear to explain the company's poor performance.

\* S&P Capital IQ, Accessed October 16, 2015.

1. Freedom House, 2015 *Freedom on the Net Index*, <https://freedomhouse.org/report/freedom-net/2015/mexico>.

2. RCR Wireless, 2014, World's Largest Mobile Operators, <http://www.rcrwireless.com/20140924/carriers/worlds-largest-mobile-operators-tag2>.

América Móvil only finds itself ahead of the poorest performers due to evidence of concrete whistleblower (Indicator C3) and grievance mechanisms (C6) in relation to privacy. However, these mechanisms do not appear to explicitly include freedom of expression issues. While it was not uncommon for telecommunications companies to provide somewhat more disclosure supporting privacy, América Móvil's failure goes beyond a simple gap on commitments to respect freedom of expression. The research could not identify evidence of relevant policy (C1) or management oversight (C2) on these issues, and there was similarly no evidence to suggest that the company performs due diligence on its business impacts (C4) or engages with relevant stakeholders in a systematic manner (C5). These are practices on which the company can certainly take steps to show improvement.

## FREEDOM OF EXPRESSION - 27%

América Móvil's score on Freedom of Expression was fourth out of eight telecommunications companies evaluated, and a full 20 percentage points behind the leading telecommunications company, Vodafone. Most of these points came from América Móvil's Mexican operating company Telcel's relatively clear and accessible terms of service (F1), its partial commitment to notify users when such policies change (F2), and its disclosure about the circumstances in which it may restrict content or access to the service (F3 and F4).

**Transparency about requests for content restriction:** The company offers no disclosure about its process for responding to any kind of request (F6) – by government or private entities – to restrict content or access to the service, nor does it publish any data about the volume or nature of any such requests (F7 and F8). While the company may face challenges disclosing such information for its operations in other markets, our understanding of Mexico's legal environment suggests that there are no legal or regulatory obstacles that prevent Telcel from disclosing its process for responding to third-party requests to restrict content – whether from the government or other third parties.

**Network management:** The company discloses that it engages in network management (F10).

## PRIVACY - 25%

América Móvil placed third among telecommunications companies on Privacy, although its score was less than half of the top scoring telecommunications company, Vodafone (52 percent), and only slightly more than half of AT&T's (49 percent). It earned only one percentage point more than Orange.

**Handling of user information:** América Móvil's Mexican operating company Telcel's disclosures about collection of mobile users' information (P3) were slightly below the full Index average, through the company's score was 20 percentage points behind the highest scoring telecommunications companies, Vodafone and AT&T. Disclosure about sharing of user information with third parties (P4) was higher than MTN and Bharti Airtel and on par with Axiata, but lower than all other telecommunications companies. Telcel tied at the front of the telecommunications cohort alongside AT&T and Vodafone for disclosing information about how users can control the company's collection of user information (P5) – albeit at a low score of 25 percent. The company provides users with no ability to access information that the company holds on them (P6), and no disclosure about the retention of user information (P7).

**Transparency about requests for user data:** When examining disclosure about the company's process for responding to third-party requests for user data (P9), América Móvil discloses a commitment to carry out due diligence on requests before deciding how to respond, but it provides no further information about its process. Beyond that, the company has no commitment to inform users about any type of requests for their information (P10). It publishes no data about the volume and nature of requests it receives (P11).

**Security:** The company discloses very little about its security practices (P12), although it does earn full points for its efforts to educate users about security threats (P14).

**AT&T, Inc.** provides telecommunications services in the United States and internationally. The company operates through two segments, Wireless and Wireline. The Wireless segment offers data and voice services to approximately 120 million wireless subscribers (as of December 2014). The Wireline segment provides telephony, Internet access, and network integration, among other services to 9 million retail consumer access lines, 9 million retail business access lines, and 2 million wholesale access lines.

**Operating company evaluated:**  
U.S.-based services

**Industry:**  
Diversified Telecommunication Services

**Services evaluated:**  
Mobile  
Fixed line broadband

**Domicile:** United States

**Market Cap:** 208,088 million\*

## OVERALL SCORE - 50%

Among telecommunications companies in this Index, AT&T ranked second only to Vodafone. Like Vodafone and Orange, AT&T is a member of the Telecommunications Industry Dialogue and has made explicit human rights commitments on freedom of expression and privacy. While its commitments and disclosures contain significant gaps – the company’s total score came out at 50 percent – it nonetheless discloses more about its policies and practices that affect users’ freedom of expression and privacy than most other telecommunications companies assessed in the Index.

## COMMITMENT - 57%

AT&T came in third place among telecommunications companies, behind Vodafone and Orange, in the Commitment category. In general, the company’s commitments are stronger on privacy than on freedom of expression. AT&T did not receive a full score on any indicator in this category, highlighting areas of improvement.

**Impact assessment:** AT&T received few points on Indicator C4, which focused on impact assessment. AT&T’s report to the Industry Dialogue explains why the company does not carry out impact assessments, stating, “Outside of the United States, AT&T primarily serves large enterprise customers, rather than the retail, consumer market. Consequently, the potential impact on users’ privacy or freedom of expression that might be associated with use of our international enterprise services is quite low.”<sup>1</sup>

Ranking Digital Rights takes the position that companies headquartered in the U.S. do, in fact, face risks that affect the freedom of expression and privacy of U.S.-based users. Therefore it is reasonable to expect companies to assess potential risks to freedom of expression and privacy associated with their business. Also, as the company notes in its most recent transparency report, in the past year AT&T expanded its business into Mexico<sup>2</sup> where freedom of expression and privacy risks to Internet users are well documented.<sup>3</sup>

\* S&P Capital IQ, Accessed October 16, 2015.

1. AT&T Telecommunications Industry Dialogue Report, [http://about.att.com/content/dam/csr/PDFs/ATT\\_Industry\\_Dialogue\\_Reporting\\_Matrix.pdf](http://about.att.com/content/dam/csr/PDFs/ATT_Industry_Dialogue_Reporting_Matrix.pdf).

2. AT&T Transparency Report, [http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT\\_Transparency%20Report\\_July%202015.pdf](http://about.att.com/content/dam/csr/Transparency%20Reports/Transparency/ATT_Transparency%20Report_July%202015.pdf).

3. Freedom House, 2015 *Freedom on the Net Index*, <https://freedomhouse.org/report/freedom-net/2015/mexico>.

**Balance of commitments:** In comments submitted to our researchers, AT&T objected to the fact that it lost credit in this category because it lacks disclosure about commitments and practices related to users' freedom of expression. A company representative stated that, until recently, AT&T provided consumer services only within the United States where, due to strong constitutional free speech protections under the First Amendment, explicit references to a company's commitments to freedom of expression are not necessary or meaningful for users.

However, the U.S. constitution's First Amendment applies only to government conduct. It does not explicitly provide protection for issues that arise related to third-party requests made to companies.<sup>4</sup> Provisions of U.S. law do limit companies' liability for the actions of users, thus enabling them to protect the free expression of their users without fear of retribution or legal action by the government or third parties (e.g., copyright holders). However, neither the law nor the constitution guarantees that a company will consider the impact of its business operations on users' freedom of expression.<sup>5</sup> It is therefore reasonable to expect companies to proactively make and demonstrate commitments to respect the freedom of expression of all users – including those residing in the United States.

## FREEDOM OF EXPRESSION - 42%

Despite the company's concerns about being judged on freedom of expression, AT&T was second only to Vodafone among telecommunications companies in the Freedom of Expression category.

**Transparency about requests for content restriction and enforcement of terms of service:** AT&T was the only telecommunications company that received any points for disclosing any data about government requests for content restriction (F7). However the company lost points on several indicators because it does not clearly disclose to users whether or how it enforces its own terms of service and how it responds to private requests, which can include content removal requests from copyright owners. For example, along with other major ISPs, AT&T is a member of the Center for Copyright Information.<sup>6</sup> The CCI website includes information about steps members may take in response to alerts received from copyright owners, including slowing Internet connection speeds and temporarily redirecting users to a landing page.<sup>7</sup> AT&T also publishes a website containing information about CCI participation<sup>8</sup>. However it does not publish data or other information about whether and to what extent it receives or responds to private requests for reasons other than copyright.

**Network management:** On Indicator F10, which examines network management practices, AT&T received partial credit for disclosing that it prioritizes or degrades content delivery, along with the purpose for doing so. Companies could only receive full credit on this indicator if they disclosed that they do not engage in such practices.

4. "Freedom of Expression in the United States," *IIP Digital*, April 17, 2013, <http://iipdigital.usembassy.gov/st/english/pamphlet/2013/04/20130416145829.html> ("The First Amendment protects citizens from *government* restrictions on free expression. It is inapplicable to situations in which a private party restricts another's speech.")

5. "Section 230 of the Communications Decency Act," *Electronic Frontier Foundation*, <https://www.eff.org/issues/cda230>; "Immunity for Online Publishers Under the Communications Decency Act," *Digital Media Law Project*, last updated February 2011, <http://www.dmlp.org/legal-guide/immunity-online-publishers-under-communications-decency-act>.

6. Center for Copyright Information: <http://www.copyrightinformation.org>.

7. See <http://www.copyrightinformation.org/the-copyright-alert-system>.

8. See <https://copyright.att.net/home>.

## PRIVACY - 52%

AT&T disclosed more about its policies and practices that affect users' privacy than any other telecommunications company in the Index. It earned leading scores on nine of the 12 privacy-related indicators on which telecommunications companies were evaluated. Nonetheless, its overall score was only a little more than half of the total possible points. Note that because the Index methodology focuses on companies' own disclosures about their practices, AT&T's score on privacy-related indicators was not directly affected by media reports based on revelations by the former intelligence contractor Edward Snowden and earlier whistleblower reports about AT&T's compliance with warrantless NSA surveillance<sup>9</sup>

**Handling of user information:** AT&T tied with Vodafone in the lead among telecommunications companies on disclosures about the collection of user information (P3), but in the Index overall it trailed 20 percentage points behind Kakao, the leading Internet company. It led the telecommunications cohort on disclosures about the sharing of user information with third parties (P4), albeit with a lackluster score of 48 percent. Its score on user control over information collection and sharing (P5) was 25 percent, tied in a very low lead with América Móvil and Vodafone plus three Internet companies. AT&T lagged behind Vodafone by a wide margin on providing users with access to their own information (P6).

On disclosures about retention of user information (P7), AT&T and five other telecommunications companies failed to receive any credit. In 2013 AT&T submitted a letter to U.S. Senator Edward J. Markey in response to a list of questions about data retention policies and law enforcement requests received.<sup>10</sup> It contained details that were not disclosed anywhere on the company's own website or in documents directed toward users. Making such information more easily available to users would improve the company's performance on several of the privacy indicators.

**Transparency about requests for user data:** AT&T's overall privacy score was boosted by the fact that it is the only telecommunications company in the Index that publishes a transparency report that includes data on the number of government requests for user data (P11). Nevertheless, the company only received 60 percent of the total possible points on this indicator. In part, this was because its transparency report lacked sufficient detail about national security requests. In company feedback, a representative objected to being penalized "for complying with clear and recently reiterated U.S. laws." However as previously noted, the Index methodology does not compensate for situations where laws prevent a company from achieving a full score on any given indicator.

On Indicators P9, P10, and P11, which examine company disclosures related to third-party requests, AT&T lost points due to a lack of information about whether and how the company receives or responds to private requests for user information. A company representative stated to researchers, "Except in emergency circumstances, we do not provide content of communications or stored data absent proper judicial or government process." However, there was no evidence that the company publicly discloses this policy in a way that users can see it. In accordance with the Index methodology, we were unable to credit the company for such a policy.

**Security:** Like Vodafone, AT&T received full marks on the Index's two security indicators (P12 and P14).

9. For example, see Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras and James Risen, "AT&T Helped U.S. Spy on Internet on a Vast Scale," *New York Times*, Aug. 15, 2015. <http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html>.

10. See [http://www.markey.senate.gov/documents/2013-10-03\\_ATT\\_re\\_Carrier.pdf](http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf).

# Axiata Group Berhad

www.axiata.com

KLSE: AXIATA

**Axiata Group Berhad** provides various telecommunication and network transmission-related services to numerous markets across Asia under various brand names. The company has approximately 240 million mobile subscribers in Asia. It operates primarily under the brands of Celcom in Malaysia, XL in Indonesia, Dialog in Sri Lanka, Robi in Bangladesh, Smart in Cambodia, Idea in India, and M1 in Singapore.

**Operating company evaluated:**  
Celcom (Malaysia)

**Industry:**  
Wireless Telecommunication Services

**Service evaluated:** Mobile

**Domicile:** Malaysia

**Market Cap:** USD 13,354 million\*

## OVERALL SCORE - 16%

Axiata's overall score was second to last among telecommunications companies, near the bottom of a cluster of four companies that scored between 14-18 percent. Malaysia was rated "Partly Free" in Freedom House's 2015 "Freedom on the Net" index.<sup>1</sup> Celcom, Axiata's subsidiary in Malaysia, is subject to the country's license, rules and regulations – many of which are not published or made available to the public.

Nonetheless, Malaysia's legal and regulatory environment does not prevent Axiata from making explicit commitments to respect users' rights and from improving its disclosure of policies and practices that affect users' freedom of expression and privacy. This commitment gap and the company's low relative performance provide a natural point of engagement for stakeholders and the company. Beyond this, and in light of the fact that regulators are known to impose content restriction in Malaysia, it is even more important that Axiata discloses its process for responding to government requests and publishes a transparency report, especially considering there are no known legal restrictions on at least minimal disclosure.

## COMMITMENT - 0%

Axiata was the only company in the Index to receive no credit for any element in this entire category. While all companies are subject to the prevailing laws and regulations in the markets in which they operate, there is no clear justification that precludes Axiata from performing better on this category. As stated above, the company's complete failure to provide relevant disclosure here provides a strong point of dialogue for engagement between stakeholders and company representatives.

\* S&P Capital IQ, Accessed October 16, 2015.

1. Freedom House, 2015 Freedom on the Net Index, <https://freedomhouse.org/report/freedom-net/2015/malaysia>



## FREEDOM OF EXPRESSION - 23%

Axiata placed fifth out of eight telecommunications companies on Freedom of Expression, although its score was less than half that of the leading telecommunications company, Vodafone. Axiata's Malaysian operating company Celcom received credit for making its terms of service available (Indicator F1), and for disclosing some information on reasons why it would restrict content or access to the service (F3 and F4).

**Transparency about requests for content restriction and enforcement of terms of service:** A major gap remained with respect to the company's policies and practices that affect freedom of expression, including enforcement of terms of service, user notification about content or account restriction, and the company's response to third-party requests to restrict content or access to the service. Malaysian laws, to our knowledge, do not limit the ability of Axiata and Celcom to disclose even general information concerning these issues. As with most jurisdictions, laws can limit company disclosures; in Axiata's case, the Malaysian Official Secrets Act 1972 may prevent it from disclosing some information about requests, but it is unrealistic that this law affects every governmental request that Axiata receives.

**Network management:** Celcom was transparent in stating that it performs network management (F10).

## PRIVACY - 17%

Axiata earned only three percentage points more than the two companies that tied for last place among telecommunications companies in this category, Etisalat and MTN. Axiata's regulatory context does not justify its lack of disclosure across the indicators assessed in this category.

**Handling of user information:** Somewhat in parallel to its performance on freedom of expression-related indicators, Axiata received credit for disclosures related to its privacy policies as well as disclosures regarding collection and sharing of user information (P3 and P4). Notably, it outperformed all telecommunications companies except AT&T and Vodafone on disclosure about collection of user information (P3), but its disclosure about sharing of user information (P4) was relatively minimal. The Malaysian operating company Celcom provides no options for users to control the collection and sharing of user information (P5), and users are given no meaningful access to their own information (P6). Such disclosure is poor despite positive regulation for data protection. For example, the Malaysian Personal Data Protection Act 2010 (PDPA) established a limit that personal data may not be kept longer than is necessary for fulfillment of the purpose for which it was collected. However, neither Axiata nor Celcom provide clarity on how this time frame is operationalized (P7).

**Transparency about requests for user data:** The company received no credit on indicators examining disclosures about its process for responding to third-party requests for user information (P9), user notification about third-party requests (P10) or data about third-party requests (P11). Notwithstanding the Official Secrets Act noted above, our understanding of Malaysian law indicates that the company should be in a position to disclose at least some types of requests that Celcom receives to share user information.

**Security:** Axiata faces no meaningful obstacles to improving its disclosures about security practices (P12), nor is there any reason why the company cannot make stronger efforts to educate users about security threats (P14).

# Bharti Airtel Limited

www.airtel.in

BSE: 532454

**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. As of March 2015, it had served approximately 324 million customers.

## Operating company evaluated:

Airtel India

## Industry:

Telecommunication Services

## Services evaluated:

Mobile  
Fixed broadband

**Domicile:** India

**Market Cap:** USD 21,584 million\*

## OVERALL SCORE - 17%

Bharti Airtel placed sixth out of eight among telecommunications companies in the Index overall. Though there are no regulatory factors that prevent Bharti Airtel from making explicit and prominent policy commitments to freedom of expression and privacy, India also does not provide any legal mechanism to incentivize companies to prioritize freedom of expression and privacy. While Indian regulations do address corporate social responsibility, their lack of explicit references to freedom of expression and privacy could help explain Bharti Airtel's failure to focus on such issues.

In 2014, the Companies Act 2013 and Corporate Social Responsibility Policy Rules 2014 were enacted. Section 135 of the Act requires companies to have CSR committees in place.<sup>1</sup> Rule 6 requires companies to have CSR policies in place, and Rule 9 requires, where possible, for policies to be displayed on the website of the company.<sup>2</sup> The Annex to the Act contains a list of activities that may be included in a company's CSR policy for a company to fulfill its CSR responsibilities. The list includes eradication of hunger and poverty, promotion of education, and reduction of child mortality, among others. It does not include freedom of expression or privacy, nor does it include a requirement to assess and address specific human rights risks associated with the company's business operations. Bharti Airtel could build on its existing CSR program and extend its company commitments, policies and practices to include freedom of expression and privacy.

## COMMITMENT - 13%

Bharti Airtel has made no overarching public commitments to protect users' freedom of expression or privacy in a manner that meets the Index's criteria. It scored fifth out of eight telecommunications companies, at the lead of a group of companies in the 0-13 percent range, while the highest-scoring companies were above 70 percent. Bharti Airtel's credit in this category was due to two factors: the presence of a whistleblower program (Indicator C3) and the highest score in the entire Index for grievance and remedy (C6).

**Remedy:** A number of legal provisions require the operating company, Airtel India, to offer different levels of redress mechanisms. Companies are required to have grievance officers in place to handle complaints pertaining to the processing of user information and the violation of laws pertaining to content prohibitions. The Telecom Regulatory Authority of

\* S&P Capital IQ, Accessed October 16, 2015.

1. Indian Companies Act 2013, section 135: <http://www.mca.gov.in/SearchableActs/Section135.htm>.

2. Companies (Corporate Social Responsibility Policies) Rules 2014, Rule 6 and Rule 9. Available at [http://www.mca.gov.in/Ministry/pdf/CompaniesActNotification2\\_2014.pdf](http://www.mca.gov.in/Ministry/pdf/CompaniesActNotification2_2014.pdf).

India also requires that all service providers have redress mechanisms.

As mentioned above, no legal impediment prevents Bharti Airtel from making top-level policy commitments to users' freedom of expression and privacy (C1), establishing executive and management oversight over these issues (C2), creating a process for human rights impact assessment (C4), or establishing and disclosing other policies described in the Commitment category.

## FREEDOM OF EXPRESSION - 16%

Bharti Airtel had the lowest score on Freedom of Expression not only among telecommunications companies but also in the entire Index. Terms of service for Airtel India's mobile and fixed broadband services were difficult to find, are available only in English (F1), and do not commit to notify users about changes to the terms of service (F2). While the company discloses what content and activities it prohibits (F3), it provides no information about how the company enforces these prohibitions. The company also discloses the circumstances under which it may suspend service to individuals or areas (F4) although it provides no examples to help users understand such policies.

**User notification about content restriction:** Bharti Airtel does not make any commitment to inform users when content has been blocked or otherwise restricted (F5). Over the past several years, researchers and journalists have identified instances in which Airtel India has provided notice when it blocks websites or pages in accordance with a court or government order. For example, one screenshot that researchers captured in 2012 on an Airtel India fixed line connection states, "this page has been blocked as per instructions from the Department of Telecommunications"<sup>3</sup> News items indicate that Airtel also blocked pages in 2014.<sup>4</sup> In order to receive credit for this indicator on the Index, Airtel India would need to disclose clear information about its policies and methods for notifying users.

**Transparency about requests for content restriction:** Regarding transparency about content restriction requests, Indian law prevents Airtel India from disclosing government requests for content removal. However, Indian law does not prevent the company from publishing more information about private requests for content restriction and as much aggregate data about all types of content restriction requests that it is permitted by law to disclose.

**Network management:** One area in which Airtel India is transparent relates to network management (F10). The company discloses the limited circumstances (excessive bandwidth use) under which it may throttle user traffic, in accordance with legal requirements.

## PRIVACY - 21%

On Privacy, Bharti Airtel places fifth out of eight telecommunications companies in the Index. While Airtel India is required by law to have a privacy policy available on its website, this policy is available in English, but not in other languages spoken in India (P1).

**Handling of user information:** Bharti Airtel scored lowest among telecommunications companies on disclosures about collection of user information (P3). Bharti Airtel received very little credit for disclosure about sharing of user information (P4) because its policies were excessively vague. The company offers no control to users about collection of their information (P5), nor does it offer users meaningful access to their information (P6). On disclosure about retention of user information (P7), Bharti Airtel ties with Vodafone at the head of the telecommunications cohort, albeit only with 20 percent. There should be no legal impediment for the company to improve its disclosures about what user information it collects, with whom it is shared, and how long it is retained.

**Transparency about requests for user data:** Several provisions in Indian law prevent disclosure of government requests to share user data or to assist with the interception of communications (P11). This appears to include aggregate

3. Blocked page screenshot from 2012. Available at <http://www.medianama.com/wp-content/uploads/Xmarks-Scrn-Shot.jpg>.

4. The Times of India, "Blocked 219 sites for infringing Sony's rights: Airtel" July 8th 2014. Accessed: October 28 2015. Available at <http://timesofindia.indiatimes.com/tech/tech-news/Blocked-219-sites-for-infringing-Sonys-rights-Airtel/articleshow/38011648.cms>

data.<sup>5</sup> However, no provisions prevent Airtel India from notifying users when a non-governmental entity requests their user data, nor are there any provisions that prevent Airtel from disclosing the types situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users (P10). The company received a zero score on Indicators P10 and P11.

**Security:** Airtel India's disclosures about its security practices earned the company only 50 percent of total possible points (P12). Its efforts to educate users about security threats (P14), however, earned full marks.

---

5. Vodafone Country by Country disclosure of law enforcement assistance demands 2015. India. Available at [http://www.vodafone.com/content/index/about/sustainability/law\\_enforcement/country\\_by\\_country.html](http://www.vodafone.com/content/index/about/sustainability/law_enforcement/country_by_country.html).

# Etisalat Group

www.etisalat.com

ADX: ETISALAT

**Etisalat Group** establishes and operates telecommunication and fiber optics networks alongside a broad suite of other services in the United Arab Emirates and in 18 other countries in the Middle East, Africa, and Asia. Its operations include operation and management of telecom networks as well as media services, connectivity services, and consulting.

**Operating company evaluated:**  
Etisalat UAE

**Industry:**  
Diversified Telecommunication Services

**Services evaluated:**  
Mobile  
Fixed broadband

**Domicile:** United Arab Emirates

**Market Cap:** USD 35,475 million\*

## OVERALL SCORE - 14%

Etisalat received the lowest overall score of all telecommunications companies evaluated in the Index. Etisalat is headquartered in a country whose legal and regulatory environment is not conducive to public commitments or disclosure on policies and practices that affect users' freedom of expression or privacy. The United Arab Emirates is rated "not free" in Freedom House's 2015 "Freedom on the Net" index.<sup>1</sup>

The country's cybercrime law, updated in 2012, holds Internet intermediaries liable for the actions of their users; it has been used to silence social media activists and justify extensive surveillance of Internet users' activities.<sup>2</sup> Overall, this context does present challenges for the company to achieve a higher score in the Index. Nevertheless, Etisalat's performance in the Index presents a potential starting point for dialogue between company representatives and stakeholders to identify where steps can be taken to provide disclosures and demonstrate a commitment to respect users' rights.

## COMMITMENT - 3%

In the Index, only one telecommunications company received a lower score than Etisalat in the Commitment category. The lone indicator on which Etisalat received any credit covered remedy and grievance mechanisms (C6). Etisalat provided avenues for users to contact the company if they had concerns about the terms of service or privacy policy, but even this disclosure left considerable room for improvement.

Etisalat operates in an environment with many legal restrictions, and the government has majority ownership of the company. The difficulty for the company to make substantive improvements in its commitment to freedom of expression and privacy in its home market nonetheless has implications for – and may potentially be of concern to – customers of the company's subsidiary operations in 18 other countries.

\* S&P Capital IQ, Accessed October 16, 2015.

1. United Arab Emirates, <https://freedomhouse.org/report/freedom-net/2015/unity-arab-emirates>.

2. "United Arab Emirates: Tracking 'cyber criminals' - Telecommunications Regulatory Authority and cyber-crime units," Enemies of the Internet, Reporters Without Borders, March 11, 2014, <http://12mars.rsf.org/2014-en/2014/03/11/unity-arab-emirates-tracking-cyber-criminals>.

## FREEDOM OF EXPRESSION - 21%

Etisalat places sixth out of eight telecommunications companies on Freedom of Expression, falling in a cluster of four companies within the 15-25 percent range. The company's credit in this category largely stems from the availability of its terms of service (F1) and disclosure about the circumstances in which it restricts content or access to the service (F3 and F4). The company's lack of disclosure concerning its process to respond to requests from any third parties dragged down its score in this category.

Within the UAE, privacy is given considerable weight, often at the expense of free expression. However, this means the law can use privacy as a means to restrict expression. A poignant example is a 2013 viral video in which an Emirati was filmed beating an Indian man. The videographer in this case was charged with defamation and invasion of privacy and would be subject to more severe penalty than the attacker.<sup>3</sup> Moreover, the country's 2012 cybercrime law holds Internet intermediaries liable for any illegal or defamatory content appearing on their websites, which restricts free expression.<sup>4</sup> In line with this legal and cultural expectation, Etisalat receives many of its points in this category on disclosures related to why it may restrict content, accounts, or service (F3 and F4).

**User notification about content restriction:** Though Etisalat does not fully commit to notify users when it restricts content or access to the service (F5), there is evidence that the company uses block pages in accordance with government requirements.<sup>5</sup>

**Network management:** Etisalat has not made public statements about its network management practices (F10). This performance gap does not appear to be the result of regulatory compliance, as there is no known law in the UAE that directs Etisalat's ability to prioritize or degrade transmission or delivery of different types of content over its network. Similarly, there is no law that limits its ability to disclose its practices in this regard.

## PRIVACY - 14%

Etisalat tied with MTN for the lowest score of any telecommunications company on Privacy. Only one company in the entire Index scored lower, the Internet company Mail.ru. Etisalat's performance showed gaps across all indicators, notably with respect to how it manages user information, how it processes requests from external parties, and how it secures its information. Especially given the premium placed on personal privacy, Etisalat has the opportunity to make basic commitments to privacy and data protections and to conduct related security audits.

**Handling of user information:** There are no obvious legal barriers against Etisalat improving its disclosure about how it handles user information. The company's disclosures about collection of user information (P3) are at the low end of the telecommunications cohort. Notably, its disclosures about the sharing of user information with third parties (P4) received the same score as Vodafone – 32 percent – surpassed only by AT&T, which scored 48 percent. There is no evidence that users can control the company's collection and sharing of their information (P5), though Etisalat scored higher than AT&T on disclosure about users' ability to access information the company holds on them (P6).

**Transparency about requests for user data:** As noted above, there is widespread understanding that the UAE's government surveils communications as part of an effort to identify political opponents or security threats. It is already established that the UAE operating context can restrict companies' ability to disclose information; furthermore, the country's penal code restricts what may be shared regarding police investigations and court trials. This, coupled with the fact that the company is majority-owned by the government, may disincentivize transparency in general, and the disclosure of law enforcement guidelines and transparency reports in particular (P9, P10, and P11). Nonetheless, the company should strive to be transparent with users about third-party requests for their information to the greatest extent possible under the law.

**Security:** It is reasonable to expect Etisalat to disclose basic information about its security practices (P12) and to publish materials that help users protect themselves from security threats (P14). The company received zero credit for either practice.

3. Matt Duffy, "Video of UAE Official Beating Indian Driver Sparks Debate," AL Monitor, July 24, 2013, <http://www.al-monitor.com/pulse/originals/2013/07/emirati-assault-video-defamation.html>.

4. UAE Cybercrime Law of 2012 <http://www.scribd.com/doc/120536757/UAE-Cybercrime-Law-of-2012>.

5. Screenshot of blockpage uploaded by Wikipedia user in August 2011: [https://en.wikipedia.org/wiki/File:Block\\_etisalat\\_3.jpg](https://en.wikipedia.org/wiki/File:Block_etisalat_3.jpg).

# MTN Group Limited

www.mtn.com

JSE: MTN

**MTN Group Limited** is a telecommunications company that serves markets in 22 countries in Africa, Asia, and the Middle East. It offers voice and data services; business services, such as cloud, infrastructure, network, software, and enterprise mobility; and mobile money and lifestyle services. As of December 2014, the company served 223.4 million subscribers.

**Operating company evaluated:**  
MTN South Africa

**Industry:**  
Wireless Telecommunication Services

**Service evaluated:** Mobile

**Domicile:** South Africa

**Market Cap:** USD 26,034 million\*

## OVERALL SCORE - 18%

MTN's overall Index score falls in a cluster of four companies in the 10-20 percent range. At the same time, South Africa's Internet is designated as "free" by Freedom House's Freedom on the Net Index.<sup>1</sup> Several factors may explain this contradiction: MTN's group-level corporate entity has historically relied on the company's operations outside of South Africa for revenue. The company operates in a number of challenging markets including Iran, Rwanda, Afghanistan, and other countries across the Middle East and North Africa, making it difficult for the company to publicly commit to respect human rights. MTN's operating companies in some markets have included government-controlled entities as shareholders. MTN also faces a few regulatory challenges at home in South Africa. Nonetheless, the company's poor performance in this Index provides a starting point for dialogue between company representatives and stakeholders to determine what concrete steps the company should take in the short- to medium-term so it can more credibly demonstrate respect for users' rights.

## COMMITMENT - 22%

MTN's public commitment to users rights was notably higher than any other telecommunications company in the Index except for the three Industry Dialogue members (Vodafone, AT&T, and Orange). However this distinction stems from the general lack of disclosure from other companies. MTN received full marks for policy and leadership (Indicator C1), which examines whether the company makes "explicit, prominent, and clearly articulated policy commitment to human rights including freedom of expression and privacy." MTN also received some credit on governance and management oversight (C2) due to its board-level oversight of how company practices affect freedom of expression and privacy. However, the company provides no further disclosure about what policies and practices it has put in place to implement its commitments.

\* S&P Capital IQ, Accessed October 16, 2015.

1. South Africa, *Freedom on the Net 2015*, Freedom House, <https://freedomhouse.org/report/freedom-net/2015/south-africa>.

## FREEDOM OF EXPRESSION - 20%

MTN scored seventh out of eight telecommunications companies in the Index on Freedom of Expression.

**Transparency about requests for content restriction:** MTN's low score is primarily due to the fact it discloses no information about the volume and nature of third-party requests that affect users' ability to access or transmit information (F7 and F8), or any information about process for responding to such requests (F6). No law in South Africa prevents MTN from disclosing general information about its processes for responding to various types of third-party requests that ask MTN to restrict content or service to users. Under South Africa's Electronic Communications and Transactions Act, MTN can lose its protection from liability if it fails to respond to requests for content removal.<sup>2</sup> Thus, the law disincentivizes companies from defending original content owners or pushing back on unlawful takedown requests. Whether it would be legal for MTN to report on government content restriction requests is unclear.

While companies in South Africa are banned from reporting on government requests for user data (as further discussed below), it is unclear whether MTN could be affected by the National Keypoints Act, which gives the government the ability to censor information about infrastructures considered crucial to national security. This could potentially prevent the company from disclosing information about requests related to content or account restriction.<sup>3</sup>

**Network management:** MTN discloses no information about whether it prioritizes or degrades the transmission or delivery of different types of content (F10). There is no "net neutrality" law in South Africa, nor does the law require MTN to disclose information about prioritizing or degrading delivery of content. MTN is under no legal obligation to monitor traffic on its network, but the law also does not prevent it from monitoring content on its network. In any case, MTN has no legal or regulatory reason why it cannot be more transparent about such practices.

## PRIVACY - 14%

MTN tied with Etisalat for the lowest score of all telecommunications companies in the Index on Privacy. Only one company in the entire Index scored lower, the Internet company Mail.ru.

**Handling of user information:** The company does a poor job of informing users about how it manages their information, for example what it collects (P3), with whom and under what circumstances it shares user information (P4), and how long it retains user information (P7). Changes in South African law may help MTN improve its performance in the future. The country's president recently signed a new Protection of Personal Information Act that requires companies to provide users with access to their own stored information, to disclose what the information is used for and explain how it is used. However the Act will not fully come into force until a Personal Information Regulator has been established, and the timeline for implementation is unknown.<sup>4</sup> In the meantime, even before the law is brought into force, there is no obstacle for MTN to meet or even exceed requirements under the new law.

**Transparency about requests for user data:** MTN provides almost no transparency about third-party requests for user information. On indicator P9, which seeks disclosure about the process for responding to third-party requests, the group level of the company commits to carry out due diligence on requests before deciding how to respond, but neither it nor the operating company provides any specifics about its process for receiving and responding to government requests or any other requests. The law prohibits the company from notifying users about requests (P10) as well as from disclosing information that pertains to the number or nature of requests (P11). In addition, the law forbids the company from

2. Alex Comminos, Intermediary liability in South Africa, Association for Progressive Communication, October 2012, <https://www.apc.org/en/pubs/intermediary-liability-south-africa>.

3. National Key Points Act, South African Government, <http://www.gov.za/documents/national-key-points-act-24-mar-2015-1016> and Philip de Wet and Chantelle Benjamin, "National Key Points: The list you weren't meant to see," *Mail and Guardian*, January 22, 2015, <http://mg.co.za/article/2015-01-22-national-key-points-the-list-you-weren't-meant-to-see>.

4. Michalsons (law firm, Nominations for Information Regulator of POPI), July 26, 2015 [www.michalsons.co.za/nominations-information-regulator-popi/15656](http://www.michalsons.co.za/nominations-information-regulator-popi/15656); Michalsons, POPI Commencement Date or POPI Effective Date, July 24, 2015, [www.michalsons.co.za/popi-commencement-date-popi-effective-date/13109](http://www.michalsons.co.za/popi-commencement-date-popi-effective-date/13109); Gregory Anderson (country manager, Trend Micro South Africa), POPI: The race to data safety, Jun 5, 2015, ITweb [www.itweb.co.za/index.php?option=com\\_content&view=article&id=143711](http://www.itweb.co.za/index.php?option=com_content&view=article&id=143711).



disclosing information about the fact that requests took place, which creates a potential problem for even disclosing information about the process for handling requests.<sup>5</sup> However there is no law preventing greater transparency about private requests.

**Security:** MTN faces no meaningful obstacles to improving its disclosures about security practices (P12), nor is there any reason why the company cannot make stronger efforts to educate users about security threats (P14).

---

5. Charlie Fripp, "SA phone companies may be used for spying, but can't tell you when," htxt.africa, June 6, 2014, <http://www.htxt.co.za/2014/06/06/sa-phone-companies-may-be-used-for-spying-but-cant-tell-you-when/>.

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

**Operating company evaluated:**

Orange (France)

**Industry**

Diversified Telecommunication Services

**Services evaluated:**

Mobile

Fixed line broadband

**Domicile:** France

**Market Cap:** USD 42,409 million\*

## OVERALL SCORE - 37%

Orange is a member of the Telecommunications Industry Dialogue and has made explicit human rights commitments on freedom of expression and privacy. It scored significantly higher than five other telecommunications companies but lagged substantially behind AT&T and Vodafone in disclosing policies and practices that affect users' rights. Orange, with operations in 29 countries in Europe and Africa (as of December 2014), faces challenges in setting policies, practices, and disclosures for its global operations given that laws differ significantly in each country<sup>1</sup>. The company receives operating licenses from governments based on its compliance with local laws. With this context in mind, we examined Orange France, the operating company in Orange's home market. While French law prevents Orange from receiving a full score on several indicators, even without changes to the legal environment in France, there is substantial room for Orange to improve its global commitments as well as policies and disclosures that pertain to Orange France.

## COMMITMENT - 73%

On Commitment, Orange came second only to Vodafone among telecommunications companies. The company could make clearer disclosures on the scope and regularity of its human rights impact assessments, as well as how the company uses the assessments (Indicator C4). The credibility of Orange's public statements about its impact assessments would improve if its assessments were externally assured and accredited to a relevant and reputable human rights standard by a credible and independent organization, such as the Global Network Initiative.

The company discloses little about its grievance and remedy process (C6). Company representatives told project researchers that while the company does track customer complaints, it does not disclose information about them. In future iterations of the Index, Orange could receive additional credit if it discloses such information to the public.

\* S&P Capital IQ, Accessed October 16, 2015.

1. Orange, 2014 Registration Document: Annual Financial Report, <http://www.orange.com/en/content/download/29884/834878/version/3/file/2014+Registration+document.pdf>.

## FREEDOM OF EXPRESSION - 29%

While Orange's disclosure related to freedom of expression is significantly better than five other telecommunications companies, it is substantially less than AT&T and Vodafone.

**Transparency about requests for content restriction:** Orange group generally, and Orange France specifically, lack transparency about policies and practices that affect users' freedom of expression. Improvements should be possible even in the current legal and regulatory context. For example the company discloses no information about its process for evaluating and responding to requests from third parties to restrict content or access to the service (F6). While operating companies in some jurisdictions may face obstacles to fulfilling this indicator, our research identified no clear legal impediment to such disclosures by Orange France.

On privacy-related requests the story is different. The company is prohibited from disclosing information about government surveillance requests (covered in the Privacy category). In many cases, it is also forbidden to disclose the web addresses or location of content that has been restricted (F5). However our research found no legal barriers to disclosing aggregate data about the *numbers of requests received to restrict content or service* (F7 and F8), or the process used to receive and consider those requests (F6). Orange can bolster the credibility of its commitment to freedom of expression by offering maximum transparency possible under the law about policies, practices, and actions that affect users' freedom of expression.

**Network management:** Orange discloses nothing about its network management practices that affect the transmission and delivery of content (F10). In communications with researchers, company representatives stated that its network management "is guided by quality of service when degrading or prioritizing the delivery of content" and that the company is compliant with French law. It is also worth noting that the E.U. is currently considering net neutrality legislation, and that as a result of this process, the regulatory situation in individual countries has been unclear. Orange may receive credit on this indicator in future iterations of the Index if it publicly discloses such information, as its peers do.

## PRIVACY - 24%

With the exception of security-focused indicators on which it performed well, Orange's disclosure on privacy related policies and practices was surprisingly poor, given its strong commitments. Notably, Orange France does not make its privacy policies publicly available at all, in stark contrast to nearly all other companies evaluated in this Index.

**Handling of user information:** Orange discloses that it is compliant with the law but often does not provide further information so that users can understand what compliance entails. For example, company representatives told our research team that the Orange follows French legal requirements related to data retention (P7), which are publicly available on a French government website. However the company does not publicly reproduce or reference this information in its own policies, and it received zero credit on P7. On disclosures about collection of user information (P3) the company was substantially outperformed by fellow Industry Dialogue members AT&T and Vodafone. Those same two companies, as well as Etisalat, surpassed Orange France on disclosure about sharing of user information (P4).

**Transparency about requests for user data:** Despite some legal obstacles, Orange should be able to improve its performance on transparency-related indicators. Orange provides no disclosure about its processes for responding to any types of third-party requests for user information (P9). While surveillance laws might be interpreted as constraining Orange's disclosure about government requests, the law does not prevent Orange from disclosing whether and how it entertains requests from non-government entities. The French Code of Criminal Procedure prevents Orange from notifying users about government surveillance (P10).

While Orange does produce a transparency report on government requests for user information (P11), it does not disclose the actual number of government requests it receives. For France it refers to a government report that discloses the total number of requests made to all operators.<sup>2</sup> However it is not possible to ascertain from such a report how many

2. See <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101/0000.pdf>.

government requests Orange received versus how many requests went to other operators. To receive credit for publishing data about third-party requests for user information, Orange would need to disclose how many requests it processes as distinct from other companies.

Also, our research was unable to identify a legal reason why the company cannot disclose to users the legal basis under which it may comply with government requests for user information, assuming that the existence of the laws themselves is not a secret. Similarly, the law does not limit the company from clarifying to users the legal circumstances that prevent it from notifying individuals about requests for user data.

**Security:** Orange received a relatively strong score for disclosing information about its security practices (P12), and it earned full marks for user education about potential threats (P14).

# Vodafone Group Plc

www.vodafone.com

LSE: VOD

**Vodafone Group Plc** operates as a telecommunications company worldwide with a significant footprint in Europe, Asia, Middle East, and Africa. It offers voice, messaging, and data services across mobile and fixed networks; fixed broadband and TV services; cloud and hosting, as well as Internet protocol-virtual private network services; roaming services; and unified communications services. The company serves 446 million mobile, 12 million fixed broadband, and 9 million TV customers.

**Operating company evaluated:**  
Vodafone UK

**Industry:**  
Wireless Telecommunication Services

**Service evaluated:** Mobile

**Domicile:** United Kingdom

**Market Cap:** USD 85,806 million\*

## OVERALL SCORE - 54%

A member of the Telecommunications Industry Dialogue, Vodafone was the top performer among telecommunications companies in the Index. The company also scored higher overall than most Internet companies, with the exception of the three founding members of the Global Network Initiative: Google, Microsoft, and Yahoo. With operations in 28 countries, Vodafone faces challenges in setting some policies, practices, and disclosures for its global operations given that laws are very different in each country, as it describes in its annual Law Enforcement Disclosure Report.<sup>1</sup> The company receives operating licenses from governments based on its compliance with local laws. Nonetheless, even for Vodafone UK, the operating company in Vodafone's home market that was evaluated in this Index, we identified a number of areas in which the company can improve its disclosures and policies within the confines of existing law.

## COMMITMENT - 75%

Among telecommunications companies, Vodafone's public commitments – and its disclosure of measures taken to implement those commitments – stood out. The company received a full score on oversight of freedom of expression and privacy (Indicator C2) and 88 percent on internal implementation of its commitments (C3). It was a relatively strong performer on impact assessments (C4), and it could boost its score further by having its assessments assured by an external third party that is accredited to a relevant and reputable human rights standard by a credible organization, such as the Global Network Initiative. Regarding remedy mechanisms, Vodafone received credit for disclosing its processes for receiving and responding to complaints or grievances (C6).

\* S&P Capital IQ, Accessed October 16, 2015.

1. See [http://www.vodafone.com/content/index/about/sustainability/law\\_enforcement.html](http://www.vodafone.com/content/index/about/sustainability/law_enforcement.html).

## FREEDOM OF EXPRESSION - 47%

Vodafone performed better than all other telecommunications companies on Freedom of Expression. The Internet companies that outperformed Vodafone in this category were Google, Kakao, Twitter, and Yahoo.

**User notification about content restriction:** Vodafone UK mobile users have documented the notices they receive when attempting to access content blocked by the service.<sup>2</sup> However the company only makes a public commitment to notify users in cases of content blocked on request of the Internet Watch Foundation, a child protection organization in the U.K. (F5). Vodafone does not commit to notify users in other cases, nor does it publish information about its approach to notification, which can only be verified by Vodafone UK subscribers when they try to access blocked content. (See further discussion of this indicator in section 4.2 of the report.)

**Transparency about requests to restrict content:** Vodafone was the only company in the entire Index to receive full marks for disclosing information about its process to evaluate and respond to requests from government and other third parties to restrict content or access to the service (F6). However the company received zero points on indicators F7 and F8, which examine whether a company discloses data about government and private third-party requests, respectively. In the U.K., where we specifically examined Vodafone's mobile service, more than one law could potentially prevent a company from disclosing specific requests to restrict content or access to a service. However, even if some U.K. laws limit Vodafone from being fully transparent, Vodafone could publish aggregate data related to all the requests it receives that it is legally allowed to publish. This would not be unprecedented. Some other U.K. companies publish the number of copyright-related blocking orders they receive, including Virgin, TalkTalk, and Sky.<sup>3</sup> Vodafone could do likewise. Moreover, other data is published in other areas, such as the terrorist-related sites blocked upon request of the Counter Terrorism Internet Referral Unit. As the NGO Open Rights Group has documented, this material has been announced in Parliament.<sup>4</sup> Vodafone could also be expected to publish this sort of data.

**Network management:** Notably, Vodafone UK was the only telecommunications company in the Index that discloses that it does not prioritize or degrade the delivery of content in its home market (F10).

## PRIVACY - 49%

Vodafone placed second among telecommunications companies on Privacy, behind AT&T. It was outperformed by four Internet companies.

**Handling of user information:** Vodafone tied with AT&T among telecommunications companies for a 60 percent score on collection of user information (P3). The company was much less competitive on disclosure about sharing user information with third parties (P4). It also tied with others for a leading score on disclosure about user options to control the company's sharing of user information (P5). However, all companies in the Index fared poorly on that indicator, the top score being only 25 percent. Vodafone's disclosures on users' ability to access the information the company holds on them (P6) and retention of user information (P7) lagged behind several Internet companies, but it led the telecommunications cohort on these two indicators.

**Transparency about requests for user data:** Vodafone had strong, though not perfect, disclosures about its process for responding to third-party requests for user information (P9). The company lost credit for not explaining its process for handling requests by private parties. A hypothetical example of such a request would be if a corporate entity whose intellectual property was violated by a user requests information about that user without first obtaining a court order. Intellectual property holders are known to have attempted such requests in other jurisdictions with other companies. If Vodafone were to publicly disclose a policy of not accepting or considering such private requests, it would gain credit in the Index.

2. See <https://blog.torproject.org/files/www.torproject.org-vodafone.png> and <http://www.pinknews.co.uk/2015/06/08/vodafone-blocks-lgbt-community-website-and-redirects-to-ad-for-flirty-dating-website/>.

3. See <http://ipkitten.blogspot.co.uk/2015/07/500-and-counting-websites-blocked-by.html>.

4. See [https://wiki.openrightsgroup.org/wiki/Counter\\_Terrorism\\_Internet\\_Referral\\_Unit](https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit).

In the U.K., the Regulation of Investigatory Powers Act (RIPA) 2000 can preclude Vodafone from notifying users when some government entities request their data.<sup>5</sup> Provisions of other laws can also gag the company from notifying users. However RIPA does not prevent the company from clarifying practices related to requests from non-government entities.

Vodafone's Law Enforcement Disclosure Report includes extensive information on what types of government demands it is unable to disclose, separated out by country and citing relevant laws. It received credit for this on Indicator P11, which examines disclosure of data about third-party requests for user information. Vodafone also provides extensive explanations of relevant legal authorities in its operating countries. All companies throughout the sector should emulate such disclosures.

However because Vodafone does not report any information about the numbers of requests of any kind that it receives in its home market, it received a relatively low overall score on P11 compared to AT&T, the second highest-scoring telecommunications company in the Index and fellow Industry Dialogue member. In its report, Vodafone cites RIPA as the reason why it cannot provide more detail about requests. It is worth noting that Vodafone has gone on public record calling for legal reforms to allow greater transparency.<sup>6</sup> However, the NGO Open Rights Group has argued that even if the law precludes publication of details of warrants made under RIPA, this should not prevent Vodafone from publishing data pertaining to other governmental requests for access to user information not covered by RIPA.<sup>7</sup>

**Security:** Vodafone, like AT&T, received full scores on Indicators P12 and P14, which focus on security standards and informing users about cyber threats.

---

5. See <http://www.legislation.gov.uk/ukpga/2000/23/section/19>.

6. See <http://www.techweekeurope.co.uk/workspace/vodafone-transparency-surveillance-nsa-spying-136210>.

7. See <https://www.openrightsgroup.org/blog/2014/no-transparency-for-the-uk-in-vodafone-transparency-report>.

# 6. APPENDIX

---

## 6.1. Methodology

The Corporate Accountability Index is the result of three years of consultation, research, and testing.<sup>1</sup> In individual and group meetings with researchers, journalists, activists, technologists, company officials, and civil society representatives, we discussed what questions this work should answer and how this data would be helpful to people. We conducted case studies of specific countries and companies to inform our research methodology.<sup>2</sup> Based on our consultations and research, we developed three iterations of the methodology and sought public feedback on each version. Working with Sustainalytics, a leading investment research firm, we tested the third version in a pilot study of 12 companies.<sup>3</sup> Following another round of public feedback and revision, we finalized the methodology for the Index.

### The Companies

We selected eight publicly listed Internet companies and eight publicly listed telecommunications companies for review. This decision was based on several factors, including geographic reach and the diversity of markets in which the companies are headquartered and operating.

#### Internet companies:

We examined company-wide policies and disclosure related to 2-3 selected services, as specified below.

- Facebook, Inc. (USA) – Facebook, WhatsApp, Instagram
- Google, Inc. (USA) – Search, Gmail, YouTube
- Kakao Corp. (South Korea) – Daum Search, Daum Mail, KakaoTalk
- Mail.ru Group (Russia) – VKontakte, Mail.ru, Mail.ru Agent
- Microsoft Corp. (USA) – Bing, Outlook.com, Skype
- Tencent Holdings Ltd. (China) – Qzone, QQ, WeChat
- Twitter, Inc. (USA) – Twitter, Vine
- Yahoo! Inc. (USA) – Mail, Flickr, Tumblr

#### Telecommunications companies:

We examined disclosure at the parent-company level and for 1-2 selected services in each company's home jurisdiction, as specified below.

- América Móvil S.A.B. de C.V. (Mexico) – Telcel's mobile service
- AT&T, Inc. (USA) – mobile and fixed broadband service

---

1. See <https://rankingdigitalrights.org/methodology-development/>.

2. See <https://rankingdigitalrights.org/project-documents/phase-1-case-study-research/>.

3. See <https://rankingdigitalrights.org/phase-1-pilot/>.



- Axiata Group Berhad (Malaysia) – Celcom’s mobile service
- Bharti Airtel Ltd. (India) – mobile and fixed broadband service
- Etisalat Group (United Arab Emirates) – mobile and fixed broadband service
- MTN Group Ltd. (South Africa) – mobile service
- Orange (France) – mobile and fixed broadband service
- Vodafone Group Plc (United Kingdom) – mobile service

**Selection of Companies:** 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 based on Alexa ranking.<sup>4</sup> The policies and practices of selected companies, and their potential to improve, thus affects a large number of people.
- **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.

**Selection of services:** The following factors guided the selection of services:

- **Internet services:** Two or three discrete services were selected based on their comparability across companies, the size of their user base, and the 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.
- **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) postpaid and prepaid mobile service, including the reasonable expected mobile offerings of voice, text, and data services, and, in cases where it was available in the home operating market, 2) fixed broadband. Only consumer services were included.

**Consideration of company 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 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, the research process did not separate these units out for AT&T.

---

4. See <http://www.alexa.com/topsites>.

The Index methodology holds a corporation responsible for the policies and practices of a new service, subsidiary, or acquisition after an initial six-month period.

**Indicators:** The Index contains 31 indicators:

- C1-C6 focus on commitment;
- F1-F11 focus on freedom of expression, and;
- P1-P14 focus on privacy.

Internet companies were evaluated on 30 of the indicators, and telecommunications companies were evaluated on 28 of the indicators. Indicators F11, P8, and P13 only applied to Internet companies, and F10 only applied to telecommunications companies. A few elements within indicators were not applicable to certain services or types of companies. The following list identifies which indicators or elements were N/A for certain companies or services:

- F4 Element 1: N/A for telecommunications companies and search engines
- F4 Element 2: N/A for Internet companies
- F4 Element 3: N/A for search engines
- F5 Element 1: N/A for telecommunications companies and search engines
- F5 Elements 1-3: N/A for email services
- F5 Element 4: N/A for search engines
- F6: N/A for email services
- F7: N/A for email services
- F7 Element 2: N/A for search engines
- F8: N/A for email services
- F8 Element 2: N/A for search engines
- F10: N/A for Internet companies
- F11: N/A for telecommunications companies
- P8: N/A for telecommunications companies
- Elements 5-6: N/A for telecommunication companies
- P12 Element 6: N/A for search engines
- P13: N/A for telecommunications companies and search engines
- P14 Element 1: N/A for telecommunications companies and search engines

For the six commitment indicators, which focus on the degree to which the company has incorporated users' rights into their governance and operations, researchers looked for disclosure related to both freedom of expression and privacy.

**The 31 indicators contain various answer types, explained below.**

**Checklist elements** – most indicators

These indicators have a list of elements, and companies receive credit for each element they fulfill.

Example: F1. Availability of Terms of Service

Are the company's Terms of Service freely available and easy to understand?

Checklist elements (select all that apply):

1. Free: The company's terms of service (ToS) are easy to find and freely available without needing to sign up or subscribe.
2. Language: The ToS is available in the language(s) most commonly spoken by the company's users.
3. Easy to understand: The ToS are presented in an understandable manner.

**If/Then answers** - C5, P3, P4, P7, P8:

These indicators contain answer options A and B, and they use skip logic. If a company fulfilled the A answer, it received full credit. If it did not, researchers checked for information on the B answer. The B answer contains a list of elements, and companies received credit for the elements they fulfilled (similar to the checklist element indicators explained above). If a company fulfilled all B elements, it received a maximum of 80 percent of the indicator score.

Example: P7. Retention of user information

Does the company disclose how long it retains user information?

A. The company discloses that it does not retain user information.

B. If not, does the company satisfy any of the following elements?

1. The company discloses that it retains user information (not actively submitted by the user for the purpose of storage or publication) in an anonymized form.
2. The company discloses the types of user information it retains.
3. The company discloses how long it retains user information.
4. The company discloses that it deletes all user information after users terminate their account.

**Single choice** – F10, F11, P13

These indicators have a list of potential answers, and researchers selected the one that best fits the company. Answer 1 is worth full credit, subsequent answers are worth decreasing levels of partial credit, and the last answer is worth zero credit (P13 is an exception, where answers 4 and 5 are worth zero credit).

Example: P13. Encryption of users' private content (Internet companies)

Can users encrypt their own content and thereby control who has access to it?

Answer categories (select one):

1. Private user content is encrypted by default; the company itself has no access.
2. The company offers a built-in option to encrypt private content.
3. The company's terms or other policies explain that the user may deploy third party encryption technologies.
4. No disclosure.
5. The company's terms or other policies prohibit encryption.

**Two-part question** – C1 is a unique indicator in that contains two parts that must be answered. Part A and Part B are single choice questions, and each is worth a maximum of 50 percent of the total score for C1.

Example: C1. Policy and leadership

A. Does the company make explicit, prominent, and clearly articulated policy commitment to human rights including freedom of expression and privacy?

Answer categories (select one):

1. Yes
2. No

B. Do senior executives of the company make meaningful commitment to advance users' freedom of expression and privacy?

Answer categories (select one):

1. Executive-level comment: A senior executive has made statements in a prominent venue.
2. Managerial-level comment: Company managers or spokesperson(s) have made statements in a prominent venue.
3. No/insufficient evidence: Company representatives have not made related statements in a prominent venue.

**Research Process:** The Index and its results are based on publicly disclosed information. Researchers thoroughly examined company websites and documents such as annual reports and sustainability reports. One indicator (C1.B) considered media reports related to the company; in all other indicators, information found in media reports did not receive credit. Researchers examined disclosure in the language of the company’s headquarters country as well as disclosure in English.

Research for the Index was carried out jointly by Ranking Digital Rights, Sustainalytics, and a team of international researchers. Most of the research and analysis was conducted between June 1, 2015 and July 31, 2015. The final cutoff date to consider any new disclosures was October 1, 2015. The research process included the following steps:

1. **Primary research:** Researchers were assigned specific companies, and they collected information for each indicator for that company.
2. **Peer review:** A second set of researchers checked the work of the primary researchers, raised questions, and suggested changes.
3. **Reconciliation:** Researchers from RDR resolved differences between the primary research results and peer review.
4. **Company review:** Initial results from step 3 were sent to companies for comment and feedback.
5. **Horizontal review:** Researchers from RDR and Sustainalytics examined results on each indicator across all companies to ensure consistency and quality control.
6. **Revision:** RDR and Sustainalytics processed company feedback and made decisions about results.
7. **Final results:** RDR finalized the data and generated scores based on the findings.

Before the research began, we defined key terms and drafted guidance for each indicator to help researchers understand what each indicator meant and how to interpret it. We published the definitions and guidance on our website.<sup>5</sup>

## Company Engagement

Proactive and open stakeholder engagement has been a critical component of the Index’s methodology. As part of our commitment to stakeholder engagement, we communicated with companies throughout the research process.

**Open dialogue and communication:** Before the research began, we contacted all 16 companies and informed them that they were included in this year’s Index. Following a first round of research and review, we shared initial results with each company. We invited them to provide written feedback as well as additional source documents. In many cases, the research team conducted conference calls with the companies to discuss the Index, its methodology, and the initial findings. This was a valuable opportunity to maintain a dialogue with stakeholders and to establish clear understanding of how digital rights can be appropriately protected and respected.

**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 how and whether technology companies disclose policies and practices that affect users’ freedom of expression and privacy. As such, 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 for context in the narrative report, but not for scoring purposes.

**Scoring:** A company’s total score on the Index is out of 100 percent. All indicators were weighted equally, so each indicator was worth approximately 3.3 percent for Internet companies and 3.6 percent for telecommunications companies (since they were evaluated on 30 and 28 indicators, respectively).

When a company received an N/A for a certain indicator or element, its score was calculated by averaging its performance across the applicable elements/indicators. In addition, any “partial” score was worth half the possible points for a given indicator/element.

---

5. See <https://rankingdigitalrights.org/wp-content/uploads/2015/06/RDR-2015-CAI-Indicators.pdf>.

During data collection, researchers documented disclosure at the group level, operating company level (if applicable) and service level. Disclosure that was recorded at a higher level (such as “group” or “operating company”) and clearly applied to the lower levels (“operating company”, “services”) was also recorded at those lower levels. This ensured that company scores reflected actual company disclosure and performance.

For indicators C1-C5, we calculated overall company scores by averaging scores across all levels. This is because we expect companies to make human rights commitments at the highest levels and that such commitments encompass all levels of the company’s operations.

For indicator C6 and for all F and P indicators, we calculated overall company scores by averaging the service-level scores. Indicator C6 focuses on the company’s remedy and grievance mechanisms, and users who seek remedy typically look for such disclosure at the service level. Similarly, the F and P indicators focus on policies and practices that relate more directly to the use of a particular service.

Throughout this report and the Index website, companies’ scores on the three categories – commitment, freedom of expression, and privacy – as well as their indicator scores, are displayed as percentages to facilitate comparison.

## 6.2 Table of Company Results Per Indicator

The following tables show each company's score on each indicator. To download this data, which includes comments that explain each score, please visit the project website, [rankingdigitalrights.org](http://rankingdigitalrights.org).

### Performance per Indicator: Internet Companies

	FACE-BOOK	GOOGLE	KAKAO	MAIL.RU	MICRO-SOFT	TENCENT	TWITTER	YAHOO
<b>TOTAL</b>	41	65	47	13	56	16	50	58
<b>COMMIT (C)</b>	62	78	39	2	82	8	35	80
<b>FOE (F)</b>	35	68	59	23	46	19	58	53
<b>PRIVACY (P)</b>	36	57	42	11	53	17	51	52
<b>C1</b>	100	100	75	0	100	38	75	100
<b>C2</b>	56	67	33	0	100	0	50	67
<b>C3</b>	92	100	50	0	100	0	25	100
<b>C4</b>	14	72	8	0	72	0	0	89
<b>C5</b>	100	100	40	0	100	0	40	100
<b>C6</b>	10	28	30	13	20	10	20	22
<b>F1</b>	72	100	83	61	100	72	83	72
<b>F2</b>	17	56	83	0	33	0	25	33
<b>F3</b>	89	78	100	56	83	67	100	94
<b>F4</b>	33	75	100	50	100	50	100	83
<b>F5</b>	21	46	42	0	4	0	50	8
<b>F6</b>	38	97	41	0	41	0	41	53
<b>F7</b>	17	83	41	0	0	0	39	42
<b>F8</b>	0	44	47	0	0	0	39	39
<b>F9</b>	0	0	0	0	0	0	0	0
<b>F10</b>	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>F11</b>	67	100	50	67	100	0	100	100
<b>P1</b>	72	100	89	28	100	100	83	89
<b>P2</b>	17	50	61	0	17	17	50	33
<b>P3</b>	67	60	80	27	60	60	60	53
<b>P4</b>	48	24	51	11	40	48	40	51
<b>P5</b>	8	25	0	0	25	0	25	17
<b>P6</b>	58	75	0	0	46	0	38	54
<b>P7</b>	23	50	23	3	57	0	70	30
<b>P8</b>	7	7	0	0	33	0	40	30
<b>P9</b>	54	88	69	0	88	0	75	77
<b>P10</b>	44	67	33	0	67	0	67	78
<b>P11</b>	23	65	60	0	60	0	70	64
<b>P12</b>	44	73	82	39	55	0	50	67
<b>P13</b>	0	17	33	0	0	0	0	0
<b>P14</b>	42	100	8	50	92	17	50	83

## Performance per Indicator: Telecommunications Companies

	AMÉRICA MÓVIL	AT&T	AXIATA	BHARTI AIRTEL	ETISALAT	MTN	ORANGE	VODA-FONE
<b>TOTAL</b>	22	50	16	17	14	18	37	54
<b>COMMIT (C)</b>	11	57	0	13	3	22	73	75
<b>FOE (F)</b>	27	42	23	16	21	20	29	47
<b>PRIVACY (P)</b>	25	52	17	21	14	14	24	49
<b>C1</b>	0	75	0	0	0	100	100	88
<b>C2</b>	0	83	0	0	0	33	100	100
<b>C3</b>	25	88	0	25	0	0	100	88
<b>C4</b>	0	6	0	0	0	0	50	53
<b>C5</b>	0	80	0	0	0	0	80	80
<b>C6</b>	40	10	0	50	20	0	10	40
<b>F1</b>	83	83	50	17	67	67	67	83
<b>F2</b>	33	17	0	0	8	33	50	17
<b>F3</b>	67	83	67	33	67	33	92	67
<b>F4</b>	33	67	67	58	50	50	67	83
<b>F5</b>	0	33	0	0	17	17	17	17
<b>F6</b>	0	69	0	0	0	0	0	100
<b>F7</b>	0	22	0	0	0	0	0	0
<b>F8</b>	0	0	0	0	0	0	0	0
<b>F9</b>	0	0	0	0	0	0	0	0
<b>F10</b>	50	50	50	50	0	0	0	100
<b>F11</b>	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>P1</b>	83	100	67	33	83	33	0	100
<b>P2</b>	0	33	0	0	0	0	0	0
<b>P3</b>	40	60	50	30	35	40	40	60
<b>P4</b>	24	48	24	8	32	16	28	32
<b>P5</b>	25	25	0	0	0	0	0	25
<b>P6</b>	0	13	0	0	19	0	0	38
<b>P7</b>	0	0	0	20	0	0	0	20
<b>P8</b>	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>P9</b>	13	88	0	6	0	13	0	75
<b>P10</b>	0	0	0	0	0	0	0	0
<b>P11</b>	0	60	0	0	0	0	35	35
<b>P12</b>	13	100	13	50	0	13	88	100
<b>P13</b>	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>P14</b>	100	100	50	100	0	50	100	100



This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of Ranking Digital Rights content when proper attribution is provided. This means you are free to share and adapt Ranking Digital Rights' work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit [creativecommons.org](https://creativecommons.org).

If you have any questions about citing or reusing Ranking Digital Rights content, please contact us at [info@rankingdigitalrights.org](mailto:info@rankingdigitalrights.org).



