RANKING DIGITAL RIGHTS

2019 RDR CORPORATE ACCOUNTABILITY INDEX

The 2019 Ranking Digital Rights Corporate Accountability Index evaluated 24 of the world's most powerful internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy.

Contents

Executive summary

The 2019 Ranking Digital Rights Corporate Accountability Index evaluated 24 of the world's most powerful internet, mobile ecosystem, and telecommunications companies on their publicly disclosed commitments and policies affecting freedom of expression and privacy. These companies held a combined market capitalization of nearly USD 5 trillion.[1] Their products and services are used by a majority of the world's 4.3 billion internet users.[2]

New Leaders for 2019

- **Microsoft** earned first place in this year's ranking, mainly due to strong governance and consistent application of policies across all services. **Google** and **Verizon Media** (formerly Oath and originally Yahoo) are now tied for second place among internet and mobile ecosystem companies—as well as in the RDR Index overall.
- **Telefónica** shot ahead of all other telecommunications companies in 2019, disclosing significantly more than its peers about policies affecting freedom of expression and privacy. The Madrid-based multinational with operations across Latin America and Europe also made more improvements than all other companies in the RDR Index by a wide margin. **Vodafone**, which led in 2018, is now in second place, ahead of **AT&T**, which fell to third.

People have a right to know. Companies have a responsibility to show. The 2019 RDR Index evaluated 24 companies on 35 indicators examining disclosed commitments, policies, and practices affecting freedom of expression and privacy, including corporate governance and accountability mechanisms. RDR Index scores represent the extent to which companies are meeting minimum standards. Yet few companies scored above 50 percent. While the results reveal some progress, many problems have persisted since the first RDR Index was launched in 2015.

Progress: Most companies have made meaningful efforts to improve. Of the 22 companies evaluated in the previous RDR Index, 19 companies disclosed more about their commitments, policies, and practices affecting users' freedom of expression and privacy.

- **Many companies improved their privacy-related policies.** New privacy regulations in the European Union and elsewhere drove many companies to improve disclosures about their handling of user information.
- **Some companies improved their governance and oversight of risks to users.** More companies improved their public commitment to respect users' human rights,

and took steps to demonstrate oversight and accountability around risks to freedom of expression and privacy.

Persistent problems: People around the world still lack basic information about who controls their ability to connect, speak online, or access information, or who has the ability to access their personal information under what circumstances. Governments are responding to serious threats perpetrated through networked communications technologies. While some regulations have improved company disclosures, policies, and practices, other regulations have made it harder for companies to meet global human rights standards for transparency, responsible practice, and accountability in relation to freedom of expression and privacy. Even when faced with challenging regulatory environments in many countries, companies must take more affirmative steps to respect users' rights.

- **PRIVACY: Most companies still fail to disclose important aspects of how they handle and secure personal data.** Despite new regulations in the EU and elsewhere, most of the world's internet users are still deprived of basic facts about who can access their personal information under what circumstances, and how to control its collection and use. Few companies were found to disclose more than required by law.
- **GOVERNANCE: Threats to users caused or exacerbated by companies' business models and deployment of new technologies are not well understood or managed.** Most companies are not prepared to identify and mitigate risks such as those associated with targeted advertising and automated decision-making. Nor do companies offer adequate grievance and remedy mechanisms to ensure that harms can be reported and rectified.
- **EXPRESSION: Transparency about the policing of online speech remains inadequate.** As companies struggle to address the harms caused by hate speech and disinformation, they are not sufficiently transparent about who is able to restrict or manipulate content appearing on or transmitted through their platforms and services, how, and under what authority. Insufficient transparency makes it easier for private parties, governments, and companies themselves to abuse their power over online speech and avoid accountability.
- **GOVERNMENT DEMANDS: Transparency about demands that governments make of companies is also uneven and inadequate.** Companies disclosed insufficient information about how they handle government demands for access to user data, and to restrict speech. As a result, in most countries, government censorship and surveillance powers are not subject to adequate oversight to prevent abuse or maintain public accountability.

To view in-depth results and data visualizations, download the full datasets, and access related resources, news, and updates, please visit: **rankingdigitalrights.org/index2019**.

If the internet is to be designed, operated, and governed in a way that protects and respects human rights, everyone must take responsibility: companies, governments, investors, civil society organizations, and individuals—as employees of companies, as citizens of nations, as consumers of products, and as users of a global communications network.

Below are our top-line recommendations for companies and governments. More detailed recommendations can be found at the end of Chapters 3, 4, and 5. Chapter 6 proposes questions for investors to ask companies.

Recommendations for companies

Regardless of the legal environment, companies are responsible for the impact of their products, services, and business operations on human rights.[3] All companies evaluated in the RDR Index can make many improvements immediately, even in the absence of legal and policy reform.

1. Go beyond legal compliance: No legal regime covered by the RDR Index enables or requires the full range of actions companies should take to respect and protect users' human rights. For companies that are committed to respecting freedom of expression and privacy as human rights, the RDR Index indicators offer clear standards to follow.[4]

2. Be transparent: Companies should disclose comprehensive and systematic data and other information that enables users to have a clear understanding of how online speech can be restricted or manipulated, and how personal information can be accessed and used—by whom and under what authority.

3. Get serious about oversight and due diligence: Board oversight and comprehensive due diligence mechanisms are necessary to identify how freedom of expression and privacy may be affected by the company's business, and to ensure that the company works to maximize the protection of users' human rights.

4. Offer effective grievance and remedy mechanisms: Users need to be able to report harms and seek remediation when their freedom of expression or privacy rights are violated in connection with using the company's platform, service, or device.

5. Innovate for better governance of data and speech: Work with civil society, investors, and governments to create new approaches for addressing threats to individuals and societies while also protecting users' rights.

Recommendations for governments

Governments should uphold their duty to protect human rights if companies are to fully respect human rights, consistent with the U.N. Guiding Principles on Business and Human Rights.[5] Citizens must be able to hold government accountable for how it exercises power over online speech and personal data.

1. Uphold human rights standards: Strong data protection law is essential for protecting privacy. Government also has a duty to protect people from violence and crime. At the same time, all laws affecting online speech, or the use and sharing of personal data by any entity, must uphold human rights standards. Governments should not enact laws that compel companies to violate, or facilitate the violation of, users' rights to freedom of expression or privacy. Any restriction of the right to freedom of expression and opinion or the right to privacy must be prescribed by law, necessary to achieve a legitimate aim (consistent with human rights standards), and proportionate to the aim pursued.

2. Commit to robust oversight: Ensure that government power to restrict online speech or access personal data is subject to meaningful oversight against abuse of censorship and surveillance power. Without credible oversight, government measures to address harmful and malicious activities via private platforms and services, or to address other social, economic, and security challenges, will be plagued by public and industry mistrust.

3. Implement and require transparency: Publish regular and accessible data disclosing the volume, nature, and purpose of all government requests made to companies affecting users' freedom of expression and privacy. Companies should also be required by law to disclose meaningful and comprehensive information about the full range of actions companies take that may affect users' freedom of expression or privacy.

4. Require strong corporate governance: Companies should be required by law to implement board oversight, systematic internal and external reporting, and impact assessments to identify, evaluate, and mitigate potential human rights harms, including violations of users' freedom of expression and privacy.

5. Ensure adequate access to remedy: People have a right to meaningful and effective remedy, including legal recourse, when their privacy or freedom of expression rights are violated. Companies should also be required by law to provide accessible and effective grievance and remedy mechanisms.

About the Ranking Digital Rights Corporate Accountability Index

Ranking Digital Rights (RDR) produces a Corporate Accountability Index that ranks the world's most powerful internet, mobile ecosystem, and telecommunications companies on relevant commitments and policies, based on international human rights standards.

The RDR Index is a standard-setting tool aimed at encouraging companies to abide by universal human rights standards guaranteeing freedom of expression and privacy. These standards build on more than a decade of work by the human rights, privacy, and security communities, including the U.N. Guiding Principles on Business and Human Rights, which affirms that just as governments have a duty to protect human rights, companies have a responsibility to respect human rights. The RDR Index also builds on the Global Network Initiative (GNI) principles[6] and implementation guidelines, which address ICT companies' specific responsibilities towards freedom of expression and privacy in the face of government demands to restrict content or hand over user information.[7] The RDR Index further draws on a body of emerging global standards and norms around data protection, security, and access to information. The RDR Index data and analysis inform the work of human rights advocates, policymakers, and responsible investors, and are used by companies to improve their own policies and practices.

The first RDR Index was released in 2015, and ranked 16 internet and telecommunications companies.

The 2017 RDR Index ranked 22 companies, which included all of the companies evaluated in 2015 plus an additional six companies. We also added new types of services, including those that produce software and devices that we call "mobile ecosystems." As a result, we expanded the methodology to account for the potential threats to users' freedom of expression and privacy that can arise from the use of networked devices and software.[8] We further refined the methodology based on a detailed review of the raw data from the 2015 RDR Index, as well as in consultation with stakeholders from civil society, academia, the investor community, and the companies themselves.

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

To read more about our methodology development, see: **rankingdigitalrights.org/methodology-development**.

The 2019 RDR Index evaluates the same 22 companies previously evaluated, plus two new telecommunications companies (**Deutsche Telekom** and **Telenor**), and added new cloud services to the evaluation of internet and mobile ecosystem companies. The 2019 RDR Index also contains limited revisions to two indicators, aimed at addressing increasingly key issues that companies in the technology sector face. Specifically, Indicator G4—evaluating corporate disclosure of human rights due diligence—was expanded to include two new elements evaluating if companies conduct human rights risks assessments (HRIAs) associated with their use of automated decision-making technologies and with their targeted advertising policies and practices. Indicator G6 was revised and strengthened to better align with standards and expectations outlined in the U.N. Guiding Principles on Business and Human Rights.

What's ahead: Following the launch of the 2019 RDR Index, we plan to expand our methodology to address human rights harms associated with targeted advertising, algorithms, and machine learning. We will also adapt the methodology to include more company types, like powerful global platforms with core e-commerce businesses such as Amazon and Alibaba. The fifth RDR Index, with the expanded methodology and scope, will be published in 2021.

For more about our methodology and development process, see: **rankingdigitalrights.org/methodology-development/2021-revisions**.

2019 RDR Index methodology

The 2019 RDR Index measures company disclosure of policies and practices affecting users' freedom of expression and privacy. The Index methodology applies 35 indicators in three main categories: **Governance**, **Freedom of Expression**, and **Privacy**. Each category contains **indicators** measuring company disclosure for that category. Each indicator is comprised of a series of **elements** that measure company disclosure for that indicator.[9]

RDR Index categories

- **Governance**: This category contains six indicators measuring company disclosure of commitments to freedom of expression and privacy principles along with measures taken to implement those commitments across the company's global operations.[10]
- **Freedom of Expression**: This category contains 11 indicators measuring company disclosure of policies that affect users' freedom of expression.[11]
- **Privacy**: This category contains 18 indicators measuring company disclosure of policies and practices that affect users' privacy rights.[12]

Company types

While each company we examined has attributes that make it unique, for the purpose of research and scoring, we divided the 24 companies into two categories.

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

For each internet and mobile ecosystem company, we evaluated global group-level policies for relevant indicators, as well as the home-country policies applicable for up to five services, as follows:

- **Apple (U.S.):** iOS mobile ecosystem, iMessage, iCloud
- **Baidu (China):** Baidu Search, Baidu Cloud, Baidu PostBar
- **Facebook (U.S.):** Facebook, Instagram, WhatsApp, Messenger
- **Google (U.S.):** Google Search, Gmail, YouTube, Android mobile ecosystem, Google Drive
- **Kakao (South Korea):** Daum Search, DaumMail, KakaoTalk
- **Mail.Ru (Russia):** VKontakte, Mail.Ru email, Mail.Ru Agent, Mail.Ru Cloud
- **Microsoft (U.S.):** Bing, Outlook.com, Skype, OneDrive
- **Samsung (South Korea):** Samsung implementation of Android, Samsung Cloud
- **Tencent (China):** QZone, QQ, WeChat, Tencent Cloud
- **Twitter (U.S.):** Twitter, Periscope
- **Verizon Media (U.S.):** Yahoo! Mail, Tumblr
- **Yandex (Russia):** Yandex Mail, Yandex Search, Yandex Disk

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

- **América Móvil (Mexico):** Telcel (pre- and postpaid mobile, broadband)
- **AT&T (U.S.):** AT&T (pre- and postpaid mobile, broadband)
- **Axiata (Malaysia):** Celcom (pre- and postpaid mobile, broadband)
- **Bharti Airtel (India):** Airtel India (pre-and postpaid mobile, broadband)
- **Deutsche Telekom AG (Germany):** Deutsche Telekom (pre- and postpaid mobile, broadband)
- **Etisalat (UAE):** Etisalat UAE (pre- and postpaid mobile, broadband)
- **MTN (South Africa):** MTN South Africa (pre- and postpaid mobile, broadband)
- **Ooredoo (Qatar):** Ooredoo Qatar (pre- and postpaid mobile, broadband)
- **Orange (France):** Orange France (pre- and postpaid mobile, broadband)
- **Telefónica (Spain):** Movistar (pre- and postpaid mobile, broadband)
- **Telenor ASA (Norway):** Telenor (pre- and postpaid mobile, broadband)
- **Vodafone (UK):** Vodafone UK (pre- and postpaid mobile, broadband)

For more information and service level comparisons, see:
rankingdigitalrights.org/index2019/services.

What the RDR Index evaluates

Commitment to freedom of expression and privacy: We expect companies to make an explicit statement affirming their commitment to freedom of expression and privacy as human rights (G1), and to demonstrate how these commitments are institutionalized within the company. Companies should disclose clear evidence of: senior-level oversight over freedom of expression and privacy (G2); employee training and whistleblower programs addressing these issues (G3); human rights due diligence and impact assessments to identify the risks the company's products, services, and business operations might have on freedom of expression and privacy (G4); systematic and credible stakeholder engagement, ideally including membership in a multi-stakeholder organization committed to human rights principles, including freedom of expression and privacy (G5); a grievance and remedy mechanism enabling users to notify the company when their freedom of expression and privacy rights have been affected or violated in connection with the company's business, plus evidence that the company provides appropriate responses or remedies (G6).

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

Terms of service enforcement: We expect companies to clearly disclose what types of content and activities are prohibited and their processes for enforcing these rules (F3). We also expect companies to publish data about the volume and nature of content and accounts they have removed or restricted for violations to their terms (F4), and to disclose if they notify users when they have removed content, restricted a user's account, or otherwise restricted access to content or a service (F8).

Handling of user information: Companies should clearly disclose each type of user information they collect (P3), share (P4), for what purposes (P5), and for how long they retain it (P6). We also expect companies to give users control over their own information, which should include options for users to control how their information is used for advertising purposes, and turning off targeted advertising by default (P7). Companies should also allow users to obtain all of the information a company holds on them (P8)

and should clearly disclose if and how they track people across the web using cookies, widgets, or other tracking tools embedded on third-party websites (P9).

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

Identity policies: We expect companies to disclose whether they ask users to verify their identities using government-issued ID or other information tied to their offline identities (F11). The ability to communicate anonymously is important for the exercise and defense of human rights around the world. Requiring users to provide a company with identifying information presents human rights risks to those who, for example, voice opinions that do not align with a government's views or who engage in activism that a government does not permit.

Network management and shutdowns: Telecommunications companies can shut down a network, or block or slow down access to specific services on it. We expect companies to clearly disclose if they engage in practices that affect the flow of content through their networks, such as by throttling or traffic shaping (F9). We also expect companies to clearly disclose their policies and practices for handling government network shutdown demands (F10). We expect companies to explain the circumstances under which they might take such action and to report on the requests they receive and with which they comply.

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

Evaluation and scoring

Research for the 2019 RDR Index was based on company policies that were active between January 13, 2018 and February 8, 2019. New information published by companies after that date was not evaluated.

2018 RDR Index score adjustments: Some company scores from 2018 were adjusted for comparison with their 2019 evaluation. Scores were adjusted at the element level, in accordance with clarified evaluation standards that were applied in the 2018 RDR Index, or to include information not located during the 2018 RDR Index cycle, or as a result of a

re-assessment of the company's disclosure. These adjustments did not produce changes to any company position in the 2018 rankings or to any of the key findings highlighted in the 2018 RDR Index. Each score adjustment, including a detailed explanation of the reason for each change, is recorded in each company's final dataset, which is publicly available for download at: rankingdigitalrights.org/index2019/download.

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

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

Points

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

For more information on scoring, see the Appendix: **rankingdigitalrights.org/index2019/report/appendix**.

1. Introduction

The number of internet users worldwide has doubled since triumphant activists of the Arab Spring embraced social media platforms as liberators in 2011.[13] Yet, since then, organizations that track global internet freedom, press freedom, and democracy have all reported alarming declines.[14] Today, tech companies have come under much-deserved scrutiny for enabling practices that critics say threaten democracy. In April 2019 UK journalist Carole Cadwalladr even challenged the founders of some of the world's most powerful internet companies to consider whether their social media platforms "have made free and fair elections a thing of the past."[15]

While the internet and related technologies helped people circumvent traditional barriers to holding governments and powerful corporations accountable, they did not shatter as many walls as democracy and human rights activists once hoped and expected. Entirely new channels have been created for abusing power and committing crimes, in ways that we are still struggling to understand. In many places and on many issues, exercising and defending human rights has grown more difficult. Civil society is under attack and space for civic action is shrinking across much of the world—online and offline.[16]

Civil society depends on freedom of expression to research, expose, debate, and protest. Equally important is the ability to live and work without being subject to blanket surveillance that makes it impossible to investigate allegations of abuse, hold accountable those who abuse power and violate human rights, or build organizations and movements that challenge established power. As the U.N. Guiding Principles on Business and Human Rights (UNGPs) make clear, governments have a primary duty to protect these rights alongside all other human rights, while companies have a responsibility to respect them throughout all aspects of their business over which they have control.[17] Yet both are failing to protect or respect internet users' freedom of expression or privacy rights in the most fundamental ways. As the World Wide Web Foundation pointed out in November 2018: "Over 1.2 billion internet users live in countries where net neutrality is not protected, and more than 1.5 billion people live in countries with no comprehensive law on personal data protection, leaving them particularly vulnerable to increasingly common incidents involving breaches of personal data."[18]

Meanwhile, many governments are attempting to hold companies responsible when internet platforms and services are used to inspire, organize, and plan numerous unspeakable acts of hate and terror. The challenge is how to do so without censoring and surveilling billions of people at the same time. The problem is exacerbated by what the Internet Society describes as "consolidation in the internet economy" at many levels:

from provision of internet access, to cloud infrastructure, to web applications and platforms.[19] Increasingly, the design choices, business models, and policy decisions of a small handful of companies are shaping political outcomes, livelihoods, and even whether some people live or die, to a degree that can only be described as shocking to those affected—and in many cases even to the companies themselves.

Diversity and choice at all layers of the global information ecosystem are essential for an internet that supports and sustains democracy and human rights. Important policy debates are now underway about how to mitigate, stop, and even reverse the trend toward consolidation that results in less choice over how we access information or what platforms we use for public discourse. Such concentration of power is especially insidious when companies are not demonstrating a clear commitment to building an internet that supports and sustains human rights.

As the Mozilla Foundation's latest Internet Health Report underscores, the health of the internet is at a critical juncture, but the future is up to everyone. Everybody who uses the internet needs to understand the power dynamics at play in the manufacture, design, and operations of the products and services we depend upon.[20] In November 2018, on the thirtieth anniversary of the creation of the World Wide Web, Sir Tim Berners-Lee called for a new Contract for the Web "with clear and tough responsibilities for those who have the power to make it better."[21]

We could not agree more. In fact, since 2013, Ranking Digital Rights (RDR) has been working with a global network of research and advocacy partners to develop clear and tough but achievable standards of commitment, disclosure, and practice for the world's most powerful internet, mobile ecosystem, and telecommunications companies. The RDR Corporate Accountability Index tracks whether and how companies are disclosing commitments, policies, and practices affecting users' freedom of expression and privacy. For the 2019 RDR Index, we have evaluated 24 companies against 35 indicators examining different aspects of their governance, policies, and practices.

The RDR Index data can be used by civil society advocates, investors, policymakers, and companies themselves to identify where specific companies fall short in protecting users' rights and how they can improve. It can also be used as a tool to show where law and regulation need to be be improved or reformed. Some regulations are essential for protecting internet users' human rights, most notably the European Union's new data protection rules. Yet in too many countries, governments are forcing companies to commit or facilitate censorship or surveillance in violation of internet users' rights. For this reason, the 2019 RDR Index report features more detailed recommendations for governments than were offered in past reports.

People have a right to know and companies have a responsibility to show. The RDR Index is most fundamentally a benchmark of how well companies are meeting their responsibility to respect users' rights. If people lack the information necessary to understand how state and non-state actors exert power through digital platforms and

services, it is impossible not only to protect human rights—but to sustain open and democratic societies. Transparency is essential in order for people to know when users' freedom of expression or privacy rights are violated either directly by—or indirectly through—companies' platforms and services, let alone identify who should be held responsible.

Some leading companies are taking seriously their responsibility to respect human rights and have done much to improve since the first RDR Index was published in November 2015. We aim to highlight the success of companies that show that they understand how the protection of internet users' human rights strengthens the "shared space" upon which they and their customers depend.[22] It is equally important to ensure that companies are held accountable for failing to meet basic standards for respecting users' human rights.

A long and difficult road lies ahead before coming close to the vision we share with many others: an internet that supports and sustains human rights. Nonetheless, the 2019 RDR Index findings do offer hope. We have seen that when companies decide to improve their respect for internet users' rights, they can.

1.1 How to read this report

This report summarizes and presents the key findings from 2019 RDR Index research. Chapter 2 presents an overview of the most notable results and changes. Chapters 3-5 provide in-depth examinations of the findings of the three RDR Index categories: Governance, Freedom of Expression, and Privacy.

All three chapters include recommendations for companies and for governments. This year we are making more detailed government recommendations than in the past. Chapter 6 offers suggested questions for investors to ask companies. The Appendix provides further details about the methodology and research process. Company report cards for each of the 24 companies are offered separately as interactive web pages, as well as PDFs that can be downloaded and printed.

1.2 Explore the data and details

While this report highlights some of the main findings from the RDR Index data, it does not analyze all of the results. To view and download the full dataset, which details how every company scored on every indicator and element, and by each service, please visit the 2019 RDR Index website at: rankingdigitalrights.org/index2019/download.

1.3 Beyond the RDR Index

The 2019 RDR Index covers 24 of the world's most powerful internet, mobile ecosystem, and telecommunications companies. It excludes many companies and services that are important to people in specific countries and regions. Because our methodology and indicators are openly available online, researchers in a range of countries and cities have begun to apply the RDR Index methodology to companies that are most relevant to them. We have compiled a list of the projects that have so far published their results: rankingdigitalrights.org/adaptations.

1.4 Beyond 2019

This report is the fourth iteration of the RDR Index since 2015. Indicators used for this and previous iterations of the RDR Index focus primarily on the freedom of expression and privacy harms that can occur to individuals as a result of their use of a company's product, service, or device. However, internet, mobile ecosystem, and telecommunications companies can also endanger human rights indirectly, or contribute to the violation of the rights of entire communities or categories of people—as revealed by journalists, activists, and scholars over the past several years. Some of these harms can be traced back to targeted advertising business models, while others relate to the use of emerging technologies such as machine learning, algorithms, and artificial intelligence.

As a result, we plan to expand the RDR Index methodology to reflect some of the tougher problems that are prompting regulatory responses: hate speech, incitement to violence, live streamed acts of violence, disinformation campaigns, and more. We have already begun the process of further developing and revising the methodology to address the rapidly evolving, increasingly complex human rights threats that internet users—and their communities—face. Our work to expand and revise the methodology will continue into 2020. The fifth RDR Index will be published in 2021 with an expanded methodology and scope, following an extensive global consultation and research process.

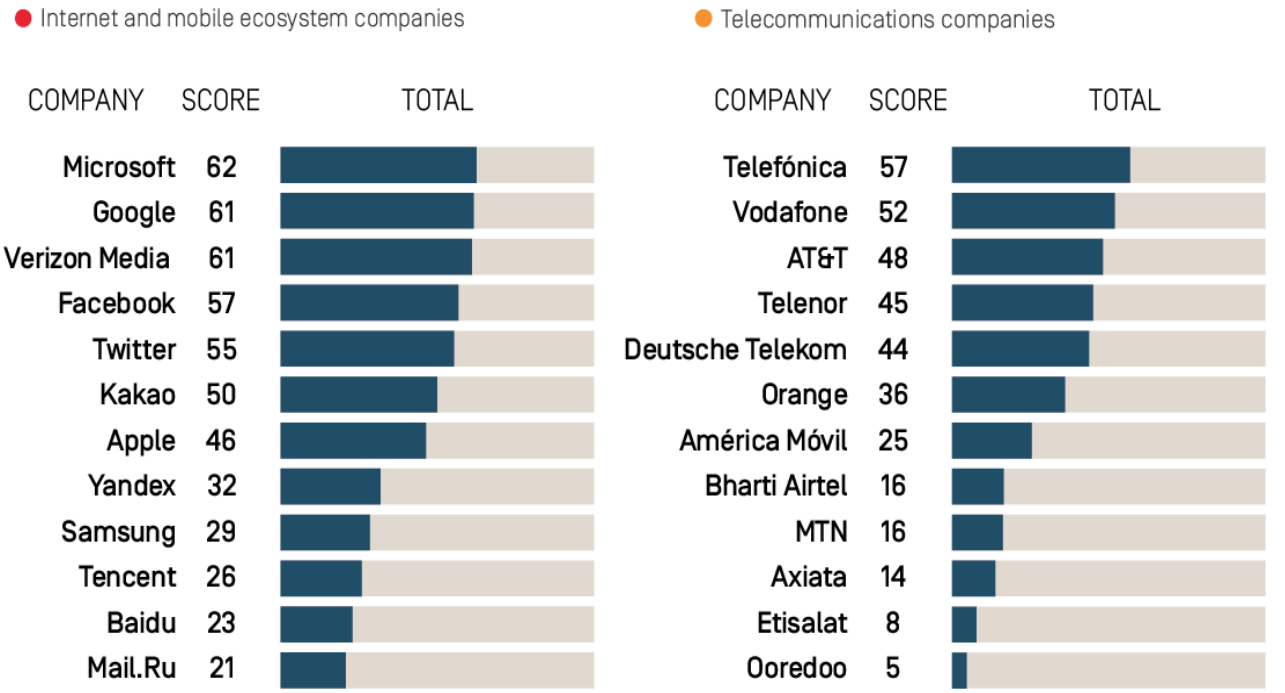
To read more about our methodology development, see: **rankingdigitalrights.org/methodology-development/2021-revisions**.

2. The 2019 RDR Index ranking: Company highlights and trends

Most companies covered by previous RDR Indexes have made tangible improvements since 2015. In the past year alone, 19 of the 22 companies that were evaluated in the 2018 RDR Index made some improvements. Yet all continue to fall short in disclosing basic information to users about the design, management, and governance of the digital platforms and services that affect human rights around the world.

The Ranking Digital Rights Corporate Accountability Index measures companies' public commitments and disclosures against standards for disclosure, policy, and practice that companies should meet in order to demonstrate respect for users' freedom of expression and privacy rights. RDR Index scores represent the extent to which companies are meeting minimum standards. Only eight of the 24 companies evaluated scored 50 percent or higher. The highest score was just 62 percent. There is much room for improvement, even when laws are not in alignment with human rights standards, and especially when regulatory requirements lag behind marketplace realities and actual harms to users.

Figure 1 | The 2019 RDR Corporate Accountability Index ranking



The highest scoring companies demonstrated relatively strong governance and oversight of human rights. They not only made clearer commitments to users' freedom of expression as well as privacy, they also disclosed mechanisms for governance and oversight of ways that their businesses might pose risks to users' rights. Nor is it a coincidence that the top-ranking 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. GNI member companies commit to a set of principles and guidelines for their implementation, which include due diligence processes as well as transparency and accountability mechanisms.[23]

The RDR Index evaluates group-level policies for relevant indicators and up to five services, depending on company type. For a breakdown of the individual services evaluated, see: **rankingdigitalrights.org/index2019/companies**.

For more about how companies are scored, see: **rankingdigitalrights.org/index2019/report/2019-index-methodology**.

2.1 Internet and mobile ecosystem highlights

Microsoft earned first place in this year's ranking, un-seating **Google**, which previously held a diminishing lead since the first RDR Index was published in 2015. Microsoft's overall score of 62 out of a possible 100 was primarily due to strong policies and disclosures in the Governance and Privacy categories, including a number of improvements. Microsoft's policies and disclosures related to its governance and oversight of risks affecting users' freedom of expression and privacy topped all other internet and mobile ecosystem companies, beating Google's governance score by 14 percentage points. Consistent application of privacy policies across all evaluated services also earned Microsoft the highest privacy score among internet and mobile ecosystem companies, edging out Google and Apple.

Google and **Verizon Media** (formerly Oath and originally Yahoo) are now tied for second place among internet and mobile ecosystem companies, and in the RDR Index overall. This tie is primarily due to Verizon Media's much stronger showing on governance oversight and risk assessment, even though Google disclosed more information overall about its policies and practices in the Freedom of Expression and Privacy categories of the RDR Index. Verizon Media also distinguished itself as the most improved U.S.-based company in the 2019 RDR Index (see Figure 2 "Year-on-year score changes" below). Most notably, it rose from sixth to third place in the Freedom of Expression category.

Facebook maintained fourth place among internet and mobile ecosystem companies. Its weak disclosure of governance and oversight mechanisms caused it to lag behind some of the other companies. Most notably, its oversight and risk assessment mechanisms demonstrated too narrow a focus on government demands, and showed no evidence that the company conducts risk assessments on how it enforces its terms of service or uses automated decision-making and targeted ads—all of which are key factors contributing to Facebook's widely reported failure to rein in hate speech and failure to protect users from unwanted and unexpected privacy violations, among other issues.[24] Facebook scored comparatively well on its transparency reporting, publishing data about content restrictions as well as government demands for user information, though its disclosure of content restriction requests declined due to lack of clarity around the report's coverage of restrictions related to WhatsApp and Messenger. Laudably, in 2018, Facebook published its first ever Community Standards Enforcement Report with regularly updated data about the nature and volume of content it restricted due to rule violations.[25] It also improved some disclosures about how it handles user information. Facebook slightly improved its disclosure of options for people to control their own user information —an area in which it disclosed less than all other internet and mobile ecosystem companies last year—by stating that users can delete some types of user information that it collects. However, overall it disclosed less choice for users to control the collection, retention, and use of their information than all of its peers other than **Baidu** and **Mail.Ru**.

2.2 Telecommunications company highlights

Telefónica shot ahead of all other telecommunications companies in 2019, disclosing significantly more than its peers about policies affecting freedom of expression and privacy. The Madrid-based multinational with operations across Latin America and Europe also made more improvements than all other companies in the RDR Index by a wide margin (see Figure 2 "Year-on-year score changes" below). Notably, Telefónica's governance score was also the highest in the entire RDR Index. The company also disclosed more information about policies and practices affecting online expression than any other telecommunications company.

Vodafone dropped to second place after being the leading telecommunications company in 2018. It was the only other telecommunications company to score more than 50 percent overall (out of a total possible 100). **AT&T** dropped to third place among telecommunications companies, down from first in 2017, mainly due to lack of improvement (see Figure 2 below) and a relatively low governance score compared to most of its European peers.

Two new telecommunications companies were added to the RDR Index in 2019: **Telenor** of Norway and **Deutsche Telekom** of Germany, which ranked fourth and fifth,

respectively, among their peers. Deutsche Telekom scored highest in the entire RDR Index on privacy due to the strong policies and practices of its home operating company, while Telenor ranked fourth among telecommunications companies in both governance and freedom of expression. Notably, Telenor scored higher than **Orange**, the French telecommunications company and fellow GNI member by nine points. Orange's strong governance at the global group level did not make up for its much weaker disclosures related to freedom of expression and privacy at the service level in its home operating market.

To read or download a company's individual report card, see: **rankingdigitalrights.org/index2019/companies**.

2.3 Notable changes

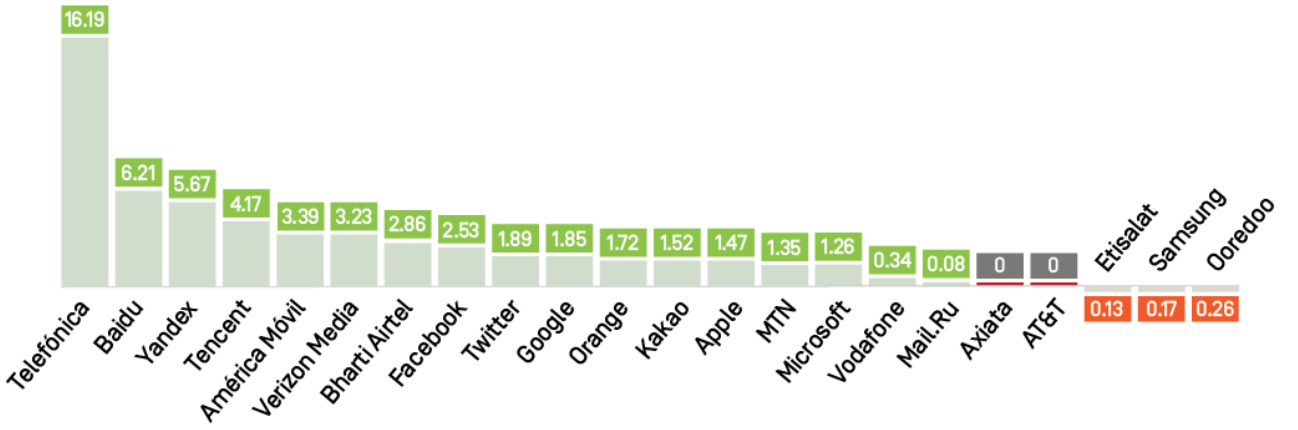
After Telefónica's dramatic 16 percentage point increase, next in line for most improved were **Baidu** of China, followed by **Yandex** of Russia, and **Tencent**, another Chinese company.

The Chinese companies' sharp improvements—mainly on some of the Privacy category indicators related to their security practices and handling of user information—appear to have been influenced by new data protection measures issued in China in May 2018.[26] Still, these companies remained near the bottom of the RDR Index: in 2019 **Tencent** ranked tenth out of 12 internet and mobile ecosystem companies, while Baidu moved up to eleventh from last place, trading places for the lowest score with Russia's **Mail.Ru**.

Yandex's improvements appeared unrelated to any Russian regulatory changes, reflecting the company's own initiative to improve. Its overall score jumped by five points, due mainly to significant improvements in the Governance category: it published a formal commitment to protect users' human rights and disclosed employee training on privacy issues. **Mail.Ru**, the other Russian company, made no notable improvements.

For details of year-on-year score changes for each company, see: **rankingdigitalrights.org/index2019/compare**.

Figure 2 | Year-on-year score changes (2018 to 2019)



While **Apple** distinguished itself in the 2018 RDR Index as the most improved company by a wide margin, in 2019 it made limited changes, primarily focusing on improving the accessibility of data about government requests to restrict accounts or hand over user information, as well as improved disclosure about encryption practices.[27] In the Privacy category, Apple tied with Google for second place behind Microsoft among internet and mobile ecosystem companies. Most notably, Apple remains the only company in the entire RDR Index that clearly disclosed that it does not track users across the internet. As discussed in Chapters 3 and 4, Apple's policies and disclosures related to freedom of expression continued to lag behind all other U.S.-based companies in the RDR Index.

América Móvil of Mexico and **Bharti Airtel** of India both made notable improvements in the past year, primarily in the Governance category, as will be further discussed in the next section.

The scores of the two companies from the Middle East and North Africa (MENA) region—**Etisalat** and **Ooredoo**—declined slightly. Ooredoo of Qatar, already ranked at the bottom of the RDR Index, did not publish any privacy policy, and received no credit in the Governance category. In second to last place Etisalat of the United Arab Emirates, which also did not publish a privacy policy, scored in the low single digits in the same two categories. Both disclosed little related to online expression other than details about what activities and types of speech are not allowed.

The other company whose score declined between 2018 and 2019 was Samsung, the South Korea-based mobile ecosystem company that uses Google's Android operating system. This decline was largely due to a decrease in transparency and clarity about its security policies and practices.

Samsung's relatively low ranking in the RDR Index stands in marked contrast with Kakao, the South Korea-based internet company which outscored Samsung by 21 percentage points in the overall RDR Index, and which earned high scores on five indicators in the Privacy category. Kakao's competitive showing in the RDR Index overall and strong disclosures and policies in key areas show that corporate accountability for users' human rights can occur in any culture or region where rule of law, freedom of the press, and civil and political rights are highly valued and well defended.

Research for the 2019 RDR Index was based on company policies that were active between January 13, 2018 and February 8, 2019. New information published by companies after February 8, 2019 was not evaluated in this year's Index. Note that some of the 2018 RDR Index scores were adjusted to align with the 2019 RDR Index evaluation.

For more about our methodology, see:
rankingdigitalrights.org/index2019/report/2019-index-methodology.

3. Governance

Companies that led the RDR Index have stronger governance. Yet governance of human rights risks faced by users remains inconsistent and uneven.

Strong governance and oversight are essential for companies to assess risks to users and mitigate harms. Without clear commitment, oversight, risk assessment, stakeholder engagement, and remedy mechanisms, even companies with good practices in certain areas—such as strong data security or robust efforts to shield users from overbroad government censorship demands—are vulnerable to serious blind spots regarding other types of risks that their users may face. Nor are they in a position to identify and mitigate harms caused by new products and technologies at a relatively early stage before they become entrenched.

While many countries are enacting new regulations focused on data protection and curbing violent extremism, the 2019 RDR Index reveals serious and persistent gaps in corporate governance that are largely unaddressed by regulators.

The Governance category of the RDR Index evaluates if companies show that they have clear processes and mechanisms in place to ensure that commitments to respect human rights—specifically freedom of expression and privacy—are made and carried out across their global business operations. A company's efforts to implement these commitments should follow, and ideally surpass, the U.N. Guiding Principles on Business and Human Rights (UNGPs), and other industry-specific human rights standards focused on freedom of expression and privacy, in particular the Global Network Initiative (GNI) Principles. Measures should include board and corporate-level oversight, internal accountability mechanisms, risk assessment, and grievance mechanisms.

The 2019 RDR Index shows that despite persistent gaps, most companies continue to make progress in this area. As was also the case between 2017 and 2018, the Governance category of the RDR Index saw the greatest overall score increase in the past year, with 11 companies making some improvements to at least one of the six indicators evaluating corporate governance of freedom of expression and privacy issues.

Evaluating corporate governance of human rights

What the RDR Index evaluates: The Governance category of the RDR Index contains six indicators that assess if companies make a clear commitment to respect and protect human rights—specifically freedom of expression and privacy—and have clear processes

and mechanisms in place to ensure that these commitments are implemented across their global business operations. Indicators evaluate:

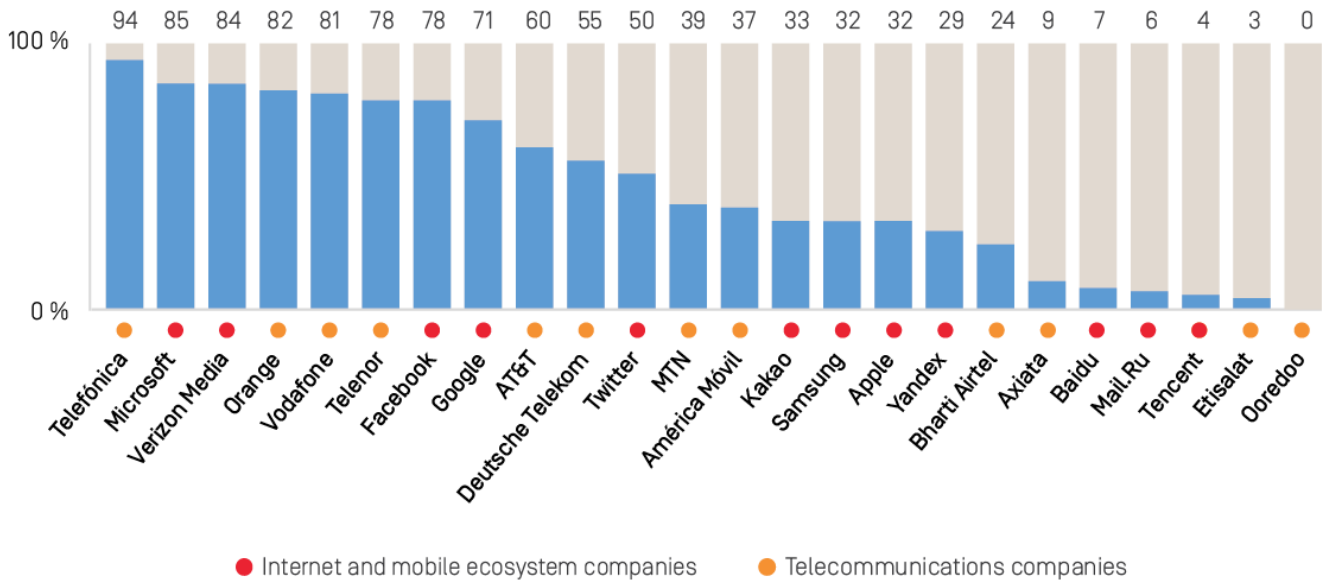
- **Human rights commitment** (G1): Does the company make an explicit statement affirming their commitment to freedom of expression and privacy as human rights?
- **Senior-level oversight** (G2): Does the company provide clear evidence of senior-level oversight over freedom of expression and privacy?
- **Internal implementation** (G3): Does the company disclose if there are employee training and whistleblower programs addressing these issues?
- **Due diligence** (G4): Does the company conduct human rights due diligence and impact assessments to identify the impacts of the company's products, services, and business operations on freedom of expression and privacy?
- **Stakeholder engagement** (G5): Does the company engage in systematic and credible stakeholder engagement, ideally including membership in a multi-stakeholder organization committed to human rights principles including freedom of expression and privacy?
- **Remedy** (G6): Does the company offer clear grievance and remedy mechanisms enabling users to notify the company when their freedom of expression and privacy rights have been affected or violated in connection with the company's business, plus evidence that the company provides appropriate responses or remedies?

See the Governance category of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#G**.

3.1 Global Network Initiative members lead the pack

As in previous iterations of the RDR Index, the top governance scores this year all went to companies that are members of GNI, a multistakeholder organization that focuses on upholding principles of freedom of expression and privacy, primarily in relation to government requests.[28] GNI-member companies commit to a set of principles and Implementation Guidelines, including implementing human rights due diligence processes as well as transparency and accountability mechanisms. Members also undergo an independent third-party assessment to verify if they are implementing these commitments, the results of which are then approved by a multistakeholder governing board made up of human rights organizations, investors, and academics, in addition to company representatives.

Figure 3 | How transparent are companies about their governance and oversight over freedom of expression and privacy?



As Figure 3 above shows, **Telefónica** earned a solid "A" in governance. The company received the top score on all six indicators in this category, disclosing more than any other company in the RDR Index about its governance and oversight over human rights issues across its global business operations. Among other areas, Telefónica stood out for its especially strong remedy mechanisms in comparison to other companies in the RDR Index (see section 3.4).

Along with **Telefónica**, GNI members **Microsoft**, **Verizon Media**, **Orange**, and **Vodafone** all disclosed strong governance of freedom of expression and privacy issues—all earning scores of over 80 percent in this category. Each of these companies disclosed a clear policy outlining a commitment to respect users' human rights, senior-level oversight over human rights issues, and internal mechanisms to implement these commitments. Orange and Verizon Media both improved their disclosure of their human rights due diligence practices.

Orange's strong performance in the Governance category stands in notable contrast to its weaker performance in other areas of the RDR Index, particularly in relation to other telecommunications companies in the GNI. A 2017 law in France requiring a "duty of vigilance" for multinational corporations means that human rights oversight and risk assessment are now mandatory for Orange.[29]

GNI member **Google** lagged behind its GNI peers for notably weaker and inconsistent governance and management of human rights commitments and policies. Google made

some progress this year by specifying that the board indeed has oversight over privacy issues (G2)—which the company had failed to clarify since re-organizing under Alphabet in 2015. But Google continued to fall significantly short of providing clear, accessible grievance and remedy mechanisms, particularly in comparison to other companies (G6).

Twitter, which is not a GNI member, disclosed almost no evidence of its human rights due diligence efforts (G4) and failed to disclose if the board oversees freedom of expression and privacy issues (G2).

Apple and **Samsung** tied at 32 percent on governance. Neither company is a GNI member. Apple's low score in this category—it was the only U.S.-based company to score under 50 percent—was due to its failure to disclose any commitments to respect freedom of expression. While Apple in 2018 took a big step forward by issuing a statement acknowledging privacy as a fundamental human right[30]—and outlining its commitment to protect that right—the company has consistently failed to recognize freedom of expression as a human right or make any commitment to protect the freedom of expression rights of its users. Given Apple's growing focus on content for revenue growth and the role of its App Store and the iTunes content platform as gatekeepers of speech, it is problematic that the company provides no evidence of governance and oversight over freedom of expression issues whatsoever (see section 3.2).

On the positive side, a handful of non-GNI-member companies took concrete steps to improve their corporate governance and oversight of human rights issues:

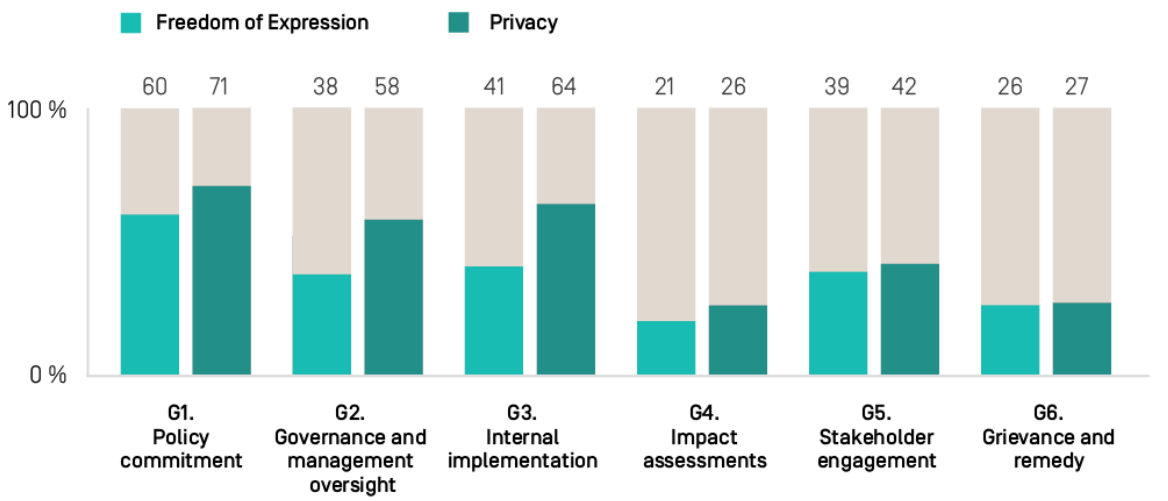
- **Yandex** took a notable step forward by publishing a clear commitment to respect the freedom of expression and privacy rights of its users.[31]
- **América Móvil** published a formal commitment to respect users' freedom of expression and privacy, and disclosed a whistleblowing program for employees to report concerns, including those related to freedom of expression and privacy violations.[32]
- **Axiata** improved its disclosure of executive-level management over privacy issues at the group level and disclosed that it has a whistleblowing mechanism for employees to report privacy violations.
- **Bharti Airtel** disclosed a commitment to protect users' human rights—although not freedom of expression or privacy specifically—and disclosed a board-level commitment to oversee privacy issues. In addition, the company improved its disclosure about its whistleblower program by clarifying that its employees can use it to report concerns over privacy related issues.

3.2 Governance gap: Expression and privacy

Most companies' corporate governance policies and practices focus on privacy risks and sideline freedom of expression.

Freedom of expression and privacy are interdependent and complementary rights. Privacy is a "gateway" to freedom of expression: it enables people to organize and discuss opinions and ideas, or to conduct research and interview sources to determine the facts of a situation prior to reporting it, without fear of retribution prior to publication.[33] Once information is shared publicly, or as it is being uploaded to a platform or transmitted through a service provider or device, it is at risk of censorship. Corporate commitment to both rights is therefore equally important. Yet most companies in the RDR Index displayed a weaker commitment to respect users' freedom of expression than to users' privacy, disclosing less oversight, due diligence, or other processes to identify and mitigate threats to users' freedom of expression.

Figure 4 | What do companies disclose about their governance and oversight over freedom of expression and privacy rights?



Average scores for all companies on their disclosed governance and oversight of the company's impact on freedom of expression and privacy across their global operations.

As Figure 4 above indicates, most companies in the RDR Index—15 out of 24—did commit to respect both freedom of expression and privacy. However, four companies—**Apple**, **Baidu**, **Kakao**, and **Tencent**—made a formal public commitment to respect users' privacy but made no similar commitment to protect freedom of expression.

As Figure 5 below shows, **Apple** had the biggest gap in its governance of freedom of expression issues as compared to privacy. It was the only company in the entire RDR Index to receive full credit for its commitment to privacy as a human right and no credit for making a similar commitment to freedom of expression. The company earned a small amount of credit on just one indicator in this category (G6)—for disclosing some

information about how app developers can file complaints if they feel that Apple has violated their freedom of expression rights if the company rejects an app from the App Store—but otherwise failed to disclose any information about its governance and oversight over freedom of expression issues at the company.

Figure 5 | Gap in governance and oversight over users' freedom of expression

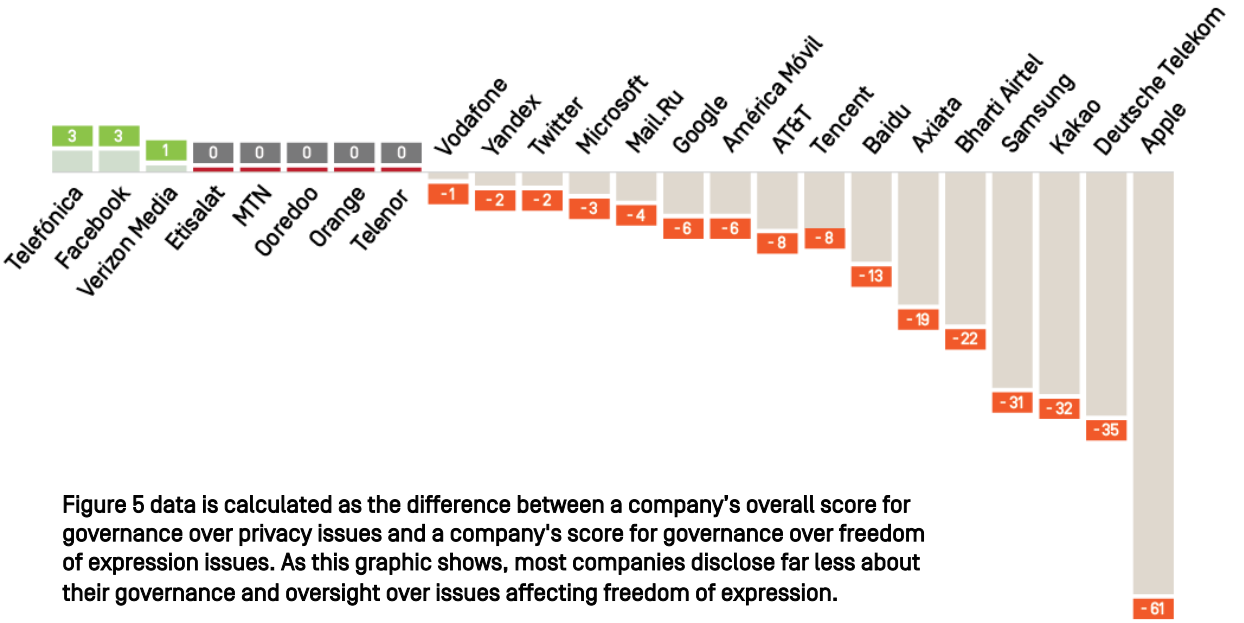


Figure 5 data is calculated as the difference between a company's overall score for governance over privacy issues and a company's score for governance over freedom of expression issues. As this graphic shows, most companies disclose far less about their governance and oversight over issues affecting freedom of expression.

Deutsche Telekom, **Kakao**, **Samsung**, **Bharti Airtel**, and **Axiata** also had noticeable gaps in their disclosure, providing far less evidence of their governance and oversight over freedom of expression commitments and policies than those related to privacy. **Deutsche Telekom** failed to disclose if there is senior-level oversight over freedom of expression issues at the company (G2) and fell short on disclosing evidence that it conducts human rights risk assessments around impacts of its business operations, products, and services on users' freedom of expression rights (G4).

Samsung and **Kakao** lacked disclosure of governance over freedom of expression in relation to privacy in similar areas: neither company disclosed any evidence of senior-level management over issues related to freedom of expression (G2), of providing employee training on these issues (G3), or of carrying out risk assessments associated with how their business operations, products, and services affect users' freedom of expression (G4).

Notably, three companies—**Facebook**, **Telefónica**, and **Verizon Media**—disclosed slightly *more* about their governance and oversight over freedom of expression as compared to their governance over privacy. **Facebook** in April 2018 launched a new appeals process for users to seek redress for wrongfully removed content, but it does not

offer a clear mechanism for users to report complaints if they feel their privacy rights have been violated by the company.

3.3 Due diligence

Few companies are prepared to anticipate human rights risks and mitigate harms.

A company that commits to respect human rights cannot credibly fulfill such a commitment without conducting regular and comprehensive assessments to understand how its products, services, and business practices affect human rights, and how any harms should be prevented or mitigated. Companies in the ICT sector that commit to respect users' freedom of expression and privacy should therefore be expected to conduct human rights risk assessments (HRIAs) on how users' rights are affected by all aspects of their business—from questions of technical design to how and where they make their services available.[34]

Indicator G4 evaluates if companies carry out regular, comprehensive, and credible due diligence, such as human rights impact assessments, in order to identify how their business operations, products, and services affect freedom of expression and privacy and to mitigate any risks posed by those impacts.[35]

Evaluating human rights due diligence

What the RDR Index evaluates: Indicator G4 evaluates if companies conduct risk assessments to evaluate and address the potential adverse impact of their business operations on users' human rights. We expect companies to carry out credible and comprehensive due diligence in order to assess and manage risks related to how their products or services may impact users' freedom of expression and privacy.

For the 2019 RDR Index, this indicator was expanded to address due diligence efforts by companies regarding their use of automated decision-making tools, as well as their targeted advertising policies and practices. Specifically, two new elements were added in order to evaluate if companies conduct risk assessments associated with their use of automated decision-making tools (such as through algorithms and artificial intelligence), and regarding their targeted advertising policies and practices.

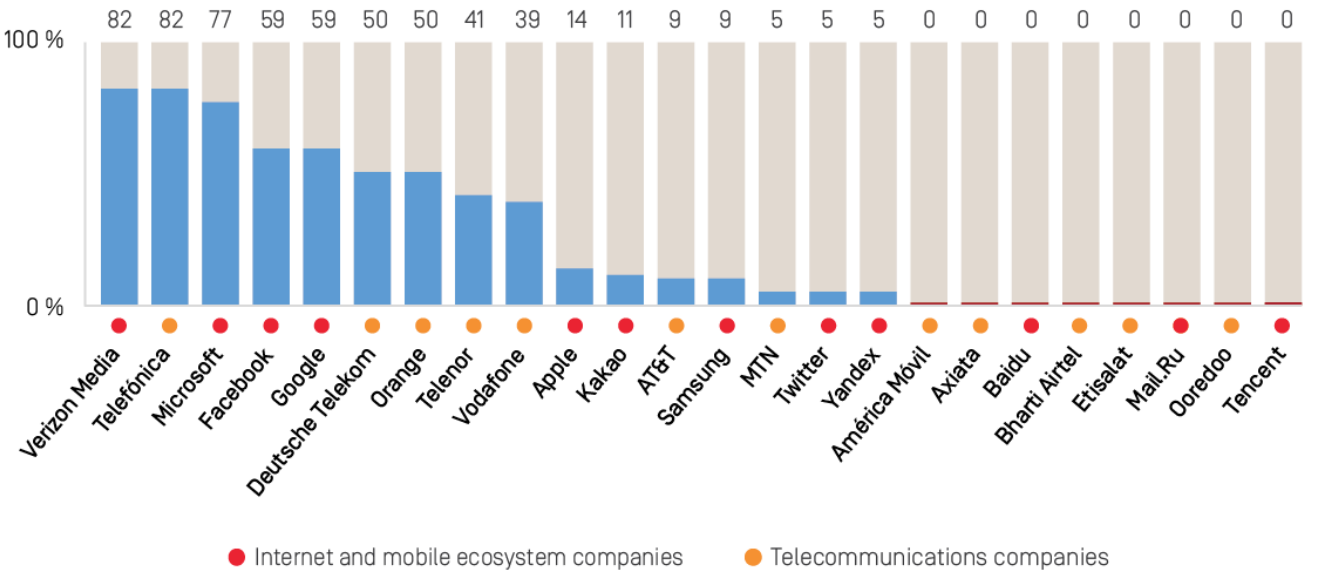
Read the guidance for Indicator G4 of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#G4**.

Few companies in the RDR Index are positioned to understand human rights risks or manage possible harms. Most of the 24 companies evaluated disclosed weak or inconsistent evidence of their human rights due diligence efforts—eight companies gave no indication that they conduct any risk assessments whatsoever.

As Figure 6 below shows, GNI-member companies disclosed more about their due diligence overall than companies that are not GNI members, but in comprehensiveness and scope, disclosure was uneven.

Telefónica and **Verizon Media** led the pack, disclosing more about their due diligence efforts than all other companies. Both companies disclosed risk assessment processes that were more comprehensive and systematic in relation to their peers: they assess risks when launching new services or entering new markets and they consider how laws in the jurisdictions where they operate might affect freedom of expression and privacy. In contrast to most other companies evaluated, Telefónica and Verizon Media disclosed that they assess risks associated with their enforcement of their terms of service, and that their assessments are conducted on a regular schedule and assured by a third party. Telefónica was one of only three companies in the RDR Index—including **Microsoft** and **Deutsche Telekom**—to disclose any information about assessing risks associated with its use of automated decision-making technologies.

Figure 6 | How comprehensive are companies' human rights impact assessments (G4)?



Apple and **Twitter**—neither of which are GNI members—provided significantly less information about their due diligence practices than their peers, making it unclear whether either company has mechanisms in place to anticipate and manage human

rights risks associated with their business operations and practices. Twitter disclosed the least information about its due diligence efforts of any U.S. company in the Index. It disclosed that its Trust and Safety team considers the impact of decisions such as entering new markets or releasing new products, but it failed to disclose whether it conducts systematic human rights impact assessments at all. Apple disclosed that it assesses the privacy risks of its existing and new products and services, but disclosed nothing about whether it assesses risks related to freedom of expression.

Most companies did not disclose if they assess risks related to their use of automated decision-making technologies, targeted advertising, or their terms of service enforcement.

As Figure 7 below shows, most companies revealed little or nothing about whether they conduct risk assessments associated with their targeted advertising policies and practices, their use of automated decision-making technologies, or their enforcement of terms of service—all key issues that have a critical and direct impact on users' human rights.

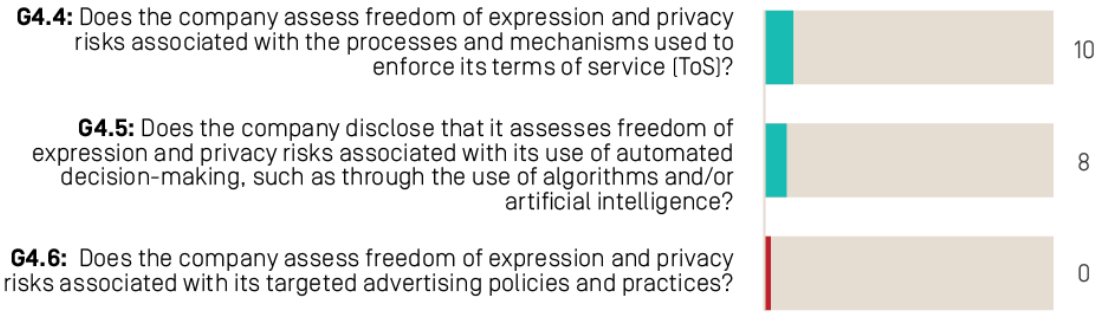
Results showed that:

- **No company clearly disclosed if it assesses risks associated with targeted advertising policies and practices.** Given the significant impact on freedom of expression and privacy that can result from companies' targeted advertising practices, the lack of evidence that any company conducts risk assessments in relation to targeted advertising has serious implications for human rights. Targeted advertising depends on the collection of vast amounts of user information so that advertisers can profile and target individuals according to specific attributes, thus incentivizing companies to track users and share their information with third parties—often without meaningful or explicit consent. Targeted advertising also incentivizes companies to manage, shape, and govern the flow of information across their networks or platforms in ways that maximize advertising revenue, which can lead to the prioritization of inflammatory content or misinformation that can infringe on freedom of expression, access to information, or incite human rights violations. Without comprehensive due diligence, companies are likely to fail to anticipate potential harm that might result from their targeted advertising policies and practices.
- Just three companies—**Deutsche Telekom**, **Microsoft**, and **Telefónica**—disclosed that they assess human rights risks associated with their use of artificial intelligence, such as through the use of algorithms or automated decision-making. Telefónica was the only company to disclose that it assesses risks associated with automated decision-making as part of its formal and ongoing human rights impact assessment process. Deutsche Telekom disclosed in its "Guidelines for artificial intelligence" that it considers the privacy risks associated with its use of AI, but did not disclose anything about assessing risks to freedom of expression. Microsoft disclosed that it

conducts human rights risk assessments regarding its development of AI technologies, but did not provide details on the scope of these assessments—such as whether the assessments cover Microsoft's use of automated decision-making in the delivery of its Bing, Skype, Outlook, or OneDrive services.[36]

- Just three companies—**Microsoft**, **Telefónica**, and **Verizon Media**—disclosed that the scope of their risk assessments include evaluating the impact of their terms of service enforcement on users' freedom of expression and privacy. Both Verizon Media and Telefónica explicitly state that they assess risks related to their terms of service as part of their formal impact assessment processes.
- No other company in the RDR Index, including **Facebook** and **Google**, offered any evidence that they conduct any sort of assessments that would enable them to identify and manage the possible adverse effects of rules enforcement on users' freedom of expression and privacy rights. Given that these two companies run platforms that regularly make headlines for issues related to whether and how they police content on their services, this gap in impact assessments has serious human rights implications.

Figure 7 | What do companies disclose about their human rights due diligence (G4)?



Indicator G4 evaluates how comprehensive companies are about their human rights due diligence practices. 2019 RDR Index data showed that most companies did not disclose if they conduct risk assessments on their terms of service enforcement, or related to their use of automated decision making technologies. No company clearly disclosed if it conducted risk assessments associated with its targeted advertising policies and practices.

3.4 Grievance and remedy

No matter how comprehensively a company assesses its human rights risks and impacts, no company is perfect. Deliberate and inadvertent harms will inevitably occur, either from the company itself or by a third-party organization. Therefore, a company

committed to respecting users' freedom of expression and privacy cannot fully meet its commitment without establishing meaningful and effective mechanisms for users to report harms and obtain redress.

Evaluating effective grievance and remedy

What the RDR Index evaluates: The RDR Index includes one indicator, G6, evaluating if companies offer clear and accessible complaints mechanisms enabling users to seek remedy if they feel their freedom of expression or privacy has been violated by the companies' actions or policies.

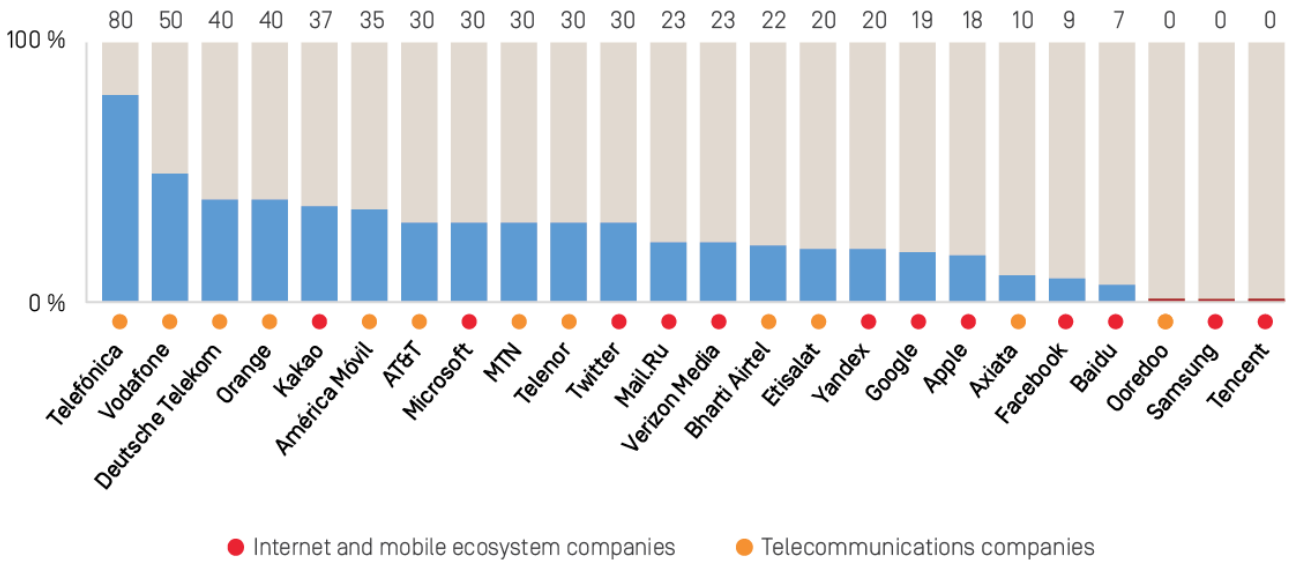
For the 2019 RDR Index, this indicator was revised in order to more closely align with the standards for remedy outlined in Principle 31 of the United Nations Guiding Principles on Business and Human Rights, which states that in order to be effective, a company's remedy procedures should be clear, accessible, predictable, and transparent. The revised Indicator G6 in the 2019 RDR Index therefore expects companies to provide users with a clear mechanism to submit grievances related to freedom of expression and privacy, to clearly disclose its remedy procedures and steps it takes to redress human rights grievances, and to offer evidence it is responding to and providing redress for these types of complaints.

Read the guidance for Indicator G6 of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#G6**.

As Figure 8 below shows, four of the five European telecommunications companies in the RDR Index—**Telefónica**, **Vodafone**, **Orange**, and **Deutsche Telekom**—earned the top scores on this indicator.

Telefónica once again had the clearest disclosure of a grievance and remedy mechanism of any company in the RDR Index, with some improvements for 2019. The company's "Responsible Business Channel"—an online portal that lets anyone file a complaint if they feel their rights have been violated—sets an example for how companies can offer a clear, accessible mechanism for users to submit human rights grievances. Telefónica also disclosed more about its processes for providing redress than any of its peers—and it was one of just five companies to disclose any evidence that it is actually responding to these complaints.

Figure 8 | Do companies provide clear and accessible grievance and remedy mechanisms to address users' freedom of expression and privacy concerns (G6)?



While GNI-member companies generally had stronger disclosure of governance and oversight over human rights issues—and therefore scored higher on this category of the RDR Index in comparison to their non-GNI member peers—this is one area where GNI membership was not a predictor of strong performance. As Figure 8 above shows, numerous non-GNI member companies—including **Kakao** and **América Móvil**—had more transparent appeals mechanisms than some GNI-member companies. Kakao's stronger disclosure was largely due to requirements under South Korean law—although Kakao went beyond the legal requirements by providing users with an appeals mechanism for when content is removed in response to defamation claims.

As we found in previous years, **Facebook's** grievance and remedy mechanisms were among the weakest of any company in the RDR Index—even after introducing improvements to its appeals process over the last year.[37] In April 2018, the company unveiled a new process for remedying wrongful takedowns of content on Facebook (the social network), but it was not clear if this mechanism covers any violation of its Community Guidelines. Meanwhile, the company lacked a clear appeal mechanism allowing users to seek remedy in cases where they feel that Facebook has violated their privacy.

Google's grievance and remedy mechanisms were slightly stronger than **Facebook's**, but still weaker than most of its peers. The company only gave options for users to appeal certain actions that could impact freedom of expression or privacy, such as copyright takedown decisions, account restrictions, or sharing user data. It was unclear

if users could submit complaints about other types of actions that a user felt infringed on their freedom of expression or privacy. Google also offered hardly any evidence that it provides effective remedy for these complaints.

3.5 Government policy and regulatory trends

Governments have a role to play in ensuring that companies exercise appropriate governance and oversight of human rights risks, including risks to users' freedom of expression and privacy.

In outlining a framework for how companies should respect human rights, the U.N. Guiding Principles on Business and Human Rights (UNGPs) emphasize the importance of commitment, oversight, stakeholder engagement, due diligence, and remedy. A growing number of governments have either published national action plans for advancing the adoption of the UNGPs by companies under their jurisdiction or have announced plans to do so.[38] Thus far, critics point out that few governments address threats to the human rights of internet users in their national action plans and the governments of many advanced economies focus narrowly on the overseas operations of their multinationals.[39]

It is nonetheless notable that some jurisdictions are starting to convert soft commitments into hard law, starting with basic reporting and disclosure requirements. The EU Non-Financial Reporting Directive, adopted in 2014, requires large companies to publish regular reports on the social and environmental impacts of their activities, including "respect for human rights."[40] All member states have transposed the directive into law.

However, analysis of company disclosures has found it to be uneven and insufficiently specific, particularly in relation to human rights due diligence.[41]

Meanwhile, laws are emerging that specifically require risk assessment. In 2017, in France, a new "duty of vigilance" law went into force for French multinationals, making strong human rights oversight and risk assessment mandatory.[42] In early 2019 the German Federal Ministry for Economic Cooperation and Development was reported to have drafted a mandatory human rights due diligence law for German companies.[43] A group of EU parliamentarians have developed an action plan for the next European Commission to draft a law requiring European companies to conduct human rights due diligence.[44] The cross-sector business and human rights movement is pushing for similar legal mandates around the world, potentially requiring companies and their investors to conduct due diligence on the full range of environmental, social, and governance (ESG) risks faced by companies in their global operations.[45]

Other jurisdictions require companies to establish grievance and remedy mechanisms through which users can lodge complaints and receive redress when their rights are violated in connection with a company's business. Indian law requires **Bharti Airtel's** domestic operating company, Airtel India, to have grievance officers as well as a redress mechanism. **Kakao's** score on remedy was bolstered by its compliance with South

Korea's data protection regime which includes the right to make complaints and seek remedies.

As the 2019 RDR Index results show, companies can certainly do much more to improve their governance of human rights risks even when governments fail to support and enable high standards of corporate respect for users' freedom of expression and privacy. U.S. companies that now disclose relatively strong governance mechanisms in relation to users' rights have done so in the absence of any regulatory requirements.

Some European companies also disclosed stronger governance than the law requires. For example: while Europe's General Data Protection Regulation (GDPR) requires EU states to appoint an independent authority to oversee privacy issues and grants every "data subject" the right to file with that authority grievances related to possible violations, companies are under no obligation under the GDPR to have or to disclose grievance and remedy procedures. There is also no obligation for companies to disclose if and how they redress human rights harms. Instead, the Spanish multinational **Telefónica**, with its relatively strong grievance and remedy mechanisms, disclosed policies consistent with its voluntary commitment to the U.N. Guiding Principles on Business and Human Rights, which stipulate that companies as well as governments have an obligation to offer channels for grievance and remedy to those whose rights have been violated in connection with the company's business.

Despite the laudable voluntary measures being taken by a number of companies, many others are failing to improve their governance of risks to users' human rights of their own accord, thus underscoring the need for thoughtful regulation requiring appropriate due diligence, oversight, and remedy.

3.6 Recommendations for companies

1. Conduct human rights impact assessments: Companies should conduct comprehensive due diligence for all aspects of their business that may affect users' human rights. These include: government and other third-party demands affecting privacy or expression, private terms of service enforcement mechanisms such as content moderation, aspects of the business model such as targeted advertising, and the application of emerging technologies such as automation and machine learning.

2. Strengthen oversight: Companies' boards of directors should exercise direct oversight over risks related to user security, privacy, and freedom of expression. To that end, board membership should include people with expertise and experience on issues related to digital rights. Boards should ensure that due diligence, remedy processes, and stakeholder engagement are effective enough to address and mitigate human rights impacts and risks.

3. Commit to third party assessment based on international human rights standards: Companies should join the Global Network Initiative or other similar multi-

stakeholder organizations that can independently assess and verify whether they are implementing their due diligence and governance processes.

4. Establish effective and accessible grievance and remedy mechanisms: These mechanisms should cover user complaints about violations of their rights to freedom of expression as well as privacy.

5. Engage with affected stakeholders: Companies should engage with those who face a high risk of human rights violations, working with these individuals and groups to co-create new processes for identifying risks, mitigating harm, receiving grievances, and providing meaningful remedy.

3.7 Recommendations for governments

1. Require company disclosure of human rights risks: Disclosures should include risks associated with their business as well as steps companies are taking to mitigate those risks.

2. Require human rights due diligence: Companies should be compelled to conduct risk assessments to identify potential human rights impacts and harms that could occur in relation to the use of the company's platform, service, or device.

3. Require effective and accessible grievance and remedy mechanisms: These mechanisms should provide meaningful legal recourse and remedy for violations of freedom of expression and privacy.

4. Assess human rights risks of new legislation: All proposed laws that may affect freedom of expression and privacy should be subject to human rights impact assessments.

4. Freedom of Expression

Across the world, a small number of internet platforms, mobile ecosystems, and telecommunications services have become powerful gatekeepers for public discourse and access to information. As discussed in Chapter 3, **Facebook**, **Google** (Youtube), and **Twitter** lack oversight and risk assessment mechanisms that could help them identify and mitigate the ways that their platforms can be used by malicious actors to organize and incite violence or manipulate public opinion. A growing body of research and scholarship has shown how these problems are exacerbated by companies' design choices and or business models.[46]

The concentrated power of a handful of companies over billions of people's online speech and access to information is causing major new social, political, and regulatory challenges to nations and communities across the world. Yet these challenges do not diminish the vital importance of freedom of expression as a fundamental human right, upon which the defense of all other rights against abuses of political and economic power ultimately depends.

Companies and civil society have documented a rapid global increase in government demands for companies to restrict and block online speech, and for telecommunications companies to throttle or even shut down internet access. Human rights law does allow for restriction of speech in a "necessary and proportionate" manner. But even democratic governments have made censorship demands of companies that fail to meet this test, which has resulted in censorship of journalists, activists, and speech by religious, ethnic, and sexual minorities.[47]

For a discussion of recent regulatory trends and challenges, see section 4.5.

How should speech be governed across globally networked digital platforms and services in a manner that supports and sustains all human rights? Solving this problem will require innovation and cooperation by and among governments, industry, and civil society, grounded in a shared commitment to international human rights principles and standards. At a time when the regulatory landscape is changing fast and in ways that threaten freedom of expression, it is vital that companies implement maximum transparency about how, why, and by whom online speech and access to information is shaped and controlled. Companies can and must do better.

4.1 Transparency remains inadequate

Transparency about how companies, governments, and other entities influence and control online expression remains inadequate.

Freedom of expression online can be restricted in a number of ways. A government can make direct demands of companies that content be removed or blocked, that a user's account be deactivated or restricted, that entire applications be removed from an app store or blocked by an internet service provider, or that entire networks be shut down. Private organizations or individuals can use legal mechanisms such as copyright infringement notices or "right to be forgotten" claims in the European Union. Companies also restrict speech when they enforce their own private terms of service. People's rights to freedom of expression are violated when a country's laws governing speech are not in alignment with international human rights standards, when government officials abuse power to censor without oversight, when enforcement is overbroad, or when individuals abuse legal mechanisms intended for the protection of their own rights to silence critics.[48]

Evaluating how transparent companies are about policies and practices affecting freedom of expression

What the RDR Index evaluates: The RDR Index evaluates company disclosure of policies and practices affecting freedom of expression across 11 indicators. Indicators assess:

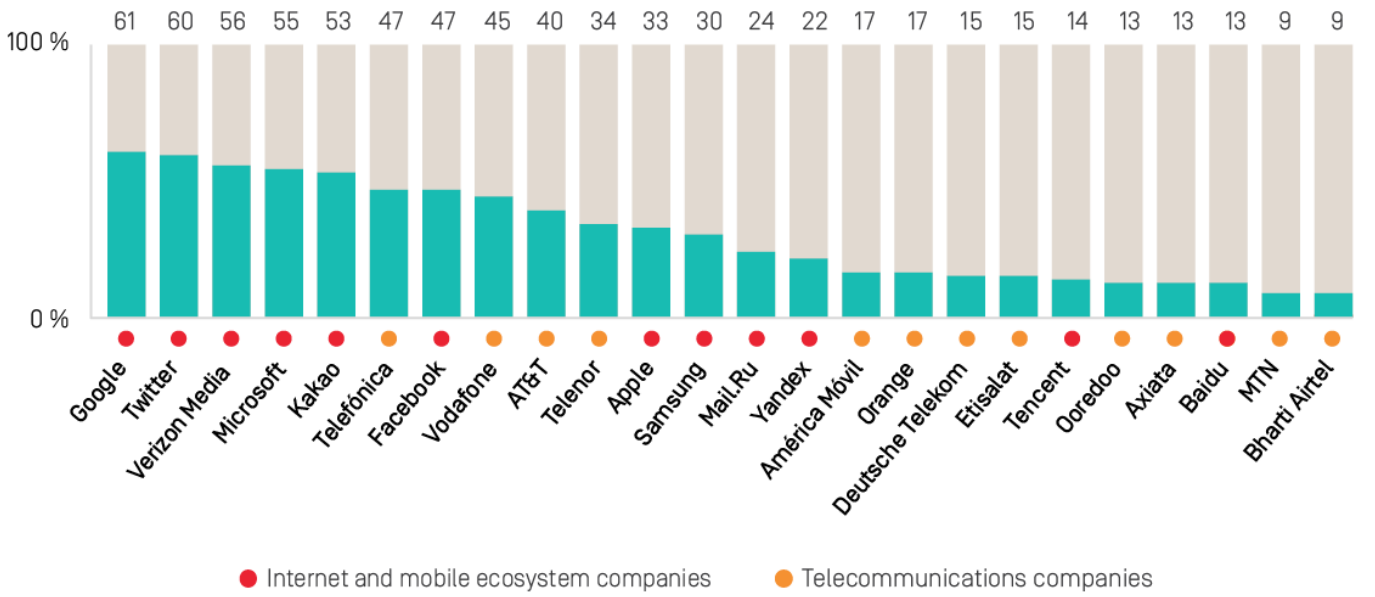
- **Accessibility and clarity of terms:** Does the company provide terms of service that are easy to find and understand? Does the company commit to notify users when they make changes to these terms (F1, F2)?
- **Content and account restrictions:** How transparent is the company about the rules and its processes for enforcing them (F3-F4)? Do companies inform users when content has been removed or accounts have been restricted, and why? (F8)
- **Government and third-party demands:** How transparent is the company about its handling of government and other types of third-party requests to restrict content or accounts (F5-F7)?
- **Network management and shutdowns (for telecommunications companies):** Does the company commit to practice net neutrality (F9)? Does the company disclose its process for handling government requests to shut down a network (F10)?
- **Identity policies**: Does the company require users to verify their identities with a government-issued ID (F11)?

The Freedom of Expression category of the RDR Index expects companies to disclose their policies and practices affecting users' speech, including how they respond to government and other types of third-party demands, as well as how they determine, communicate, and enforce private rules and commercial practices that affect users' freedom of expression.

Companies' average overall performance in the Freedom of Expression category increased only slightly between 2018 and 2019. This means that internet users still lack adequate information about how their speech or access to information may be restricted, by whom, under what authority or circumstances.

A handful of internet companies took major steps forward in boosting transparency about the volume and nature of content and accounts that were deleted or restricted when enforcing their own terms of service. **Google** boosted its overall freedom of expression score primarily for this reason (see section 4.2). Yet others took steps backward that exceeded their steps forward. While Facebook made some significant improvements in transparency about terms of service enforcement, as will be discussed below, its overall freedom of expression score nonetheless declined due to decreased transparency in relation to third-party and government demands.

Figure 9 | How transparent are companies about policies and practices affecting freedom of expression (F1 - F11)?



One telecommunications company, **Telefónica**, made major strides in transparency about government and third-party demands affecting users' freedom of expression in particular. But with the exception of slight improvements by **MTN** and **Axiata**, all other telecommunications companies were either stagnant or backtracked. Notably, **Vodafone**, which ranked high overall and improved in the other categories, backtracked slightly in freedom of expression due to reduced clarity about its rules and their enforcement.

4.2 Terms of service and enforcement

While a few companies took laudable steps by publishing data about the volume and nature of content removed for violating terms of service, none disclosed enough about their rules or actions taken to enforce them—and most disclosed nothing.

When the inaugural RDR Index launched in 2015, no company received any credit on the indicator measuring whether they regularly publish data about the volume and nature of actions taken to restrict content or accounts that violate the company's rules (F4).

While most companies in the RDR Index still failed to earn any credit on this indicator, three companies—**Facebook**, **Google**, and **Twitter**—made significant strides by publishing comprehensive data about content removals due to terms of service enforcement, while another company, Microsoft, published some information, albeit in a less systematic manner.

Evaluating how transparent companies are about actions they take to enforce their terms of service

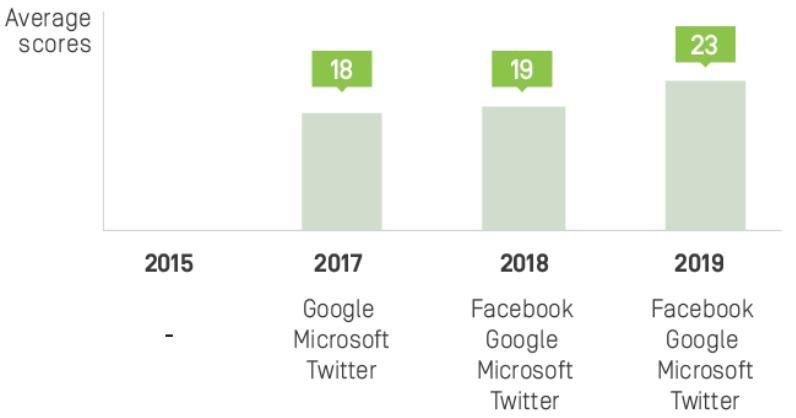
What the RDR Index measures: Indicator F4 of the RDR Index evaluates if companies clearly disclose and regularly publish data about the volume and nature of actions taken to restrict content or accounts that violate the company's rules.

- **Element 1**: Does the company clearly disclose data about the volume and nature of content and accounts restricted for violating the company's rules?
- **Element 2:** Does the company publish this data at least once a year?
- **Element 3:** Can the data published by the company be exported as a structured data file?

Read the guidance for Indicator F4 of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#F4**.

Facebook, **Google**, and **Twitter** all published more data about content removals due to terms of service enforcement than they had previously. In May 2018, Facebook published a new Community Standards Enforcement Report with more comprehensive data on terms of service enforcement for the social network. Shortly before that, in April 2018, Google released its first Community Guidelines Enforcement Report for YouTube, with more comprehensive data regarding the nature and volume of removals due to terms of service enforcement. Twitter took a step forward by publishing, in December 2018, a single, comprehensive report focused on terms of service enforcement, which included data on the number of accounts it took action against and for what category of violation.

Figure 10 | How transparent are companies about terms of service enforcement (2015-2019)?



Indicator F4 evaluates if companies disclose data about the volume and nature of content or accounts they remove or restrict for rules violations. Most companies disclose nothing at all. Four companies disclose some data although the information they provide is inconsistent and often incomplete.

Average scores for companies that earned any points on this indicator (F4).

Despite publishing more structured and comprehensive transparency reports, **Facebook**'s and **Google**'s scores on this indicator—which are calculated by averaging scores across several services—ended up lower than **Microsoft**'s, which published less comprehensive data but was more consistent across services. Facebook scored lower than Microsoft because its new Community Standards Enforcement Report applied just to Facebook (the social network) and not to Instagram, WhatsApp, or Messenger. Similarly, Google's new report applied only to YouTube. **Twitter** lost points for not supplying the data in a structured format, and because it was not clear if the company plans to regularly publish this data.

The RDR Index has three other indicators that evaluate how clear companies are about their rules and enforcement processes: if their terms are easy to find and to understand (F1), if they disclose whether they notify users of changes (F2), and if they disclose

sufficient information about what types of content or activities are prohibited and how these rules are enforced (F3).

While five companies—**Axiata**, **Facebook**, **Google**, **MTN**, and **Verizon Media**—improved the accessibility of their terms of service, **Ooredoo** and **Yandex** showed declines. (For Yandex terms were no longer easy to find and for Ooredoo not all terms for all services were available in the home market's primary languages.) Five companies—**Facebook**, **Microsoft**, **MTN**, **Verizon Media**, and **Twitter**—clarified the way they notify users when they change their terms of service, but **Vodafone**'s score declined since its postpaid mobile terms no longer disclosed a time frame for notifying users of changes.

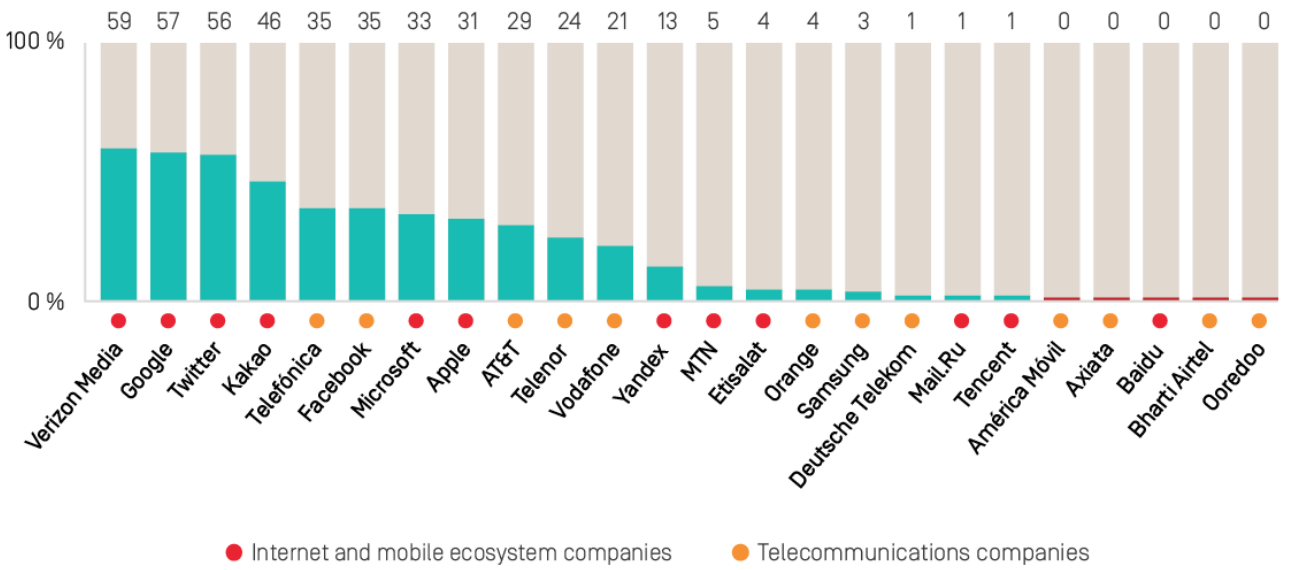
Telenor disclosed more information than any other telecommunications company about its rules and how they are enforced (F3). However, it should be noted that this is the only indicator on which all companies in the RDR Index received at least some credit. All companies published terms of service that included at least basic information about prohibited activities or content, such as rules against using their services to violate copyright laws or to harass or defame others. Companies based in jurisdictions where the law explicitly bans certain types of speech also tend to list these prohibited activities and content in their terms of service. It is for this reason, primarily, that Qatar-based **Ooredoo**—which placed last in the entire RDR Index—earned points in the Freedom of Expression category for disclosures about the content and enforcement of its rules, while earning no credit in either the Governance or Privacy categories.

4.3 External demands to restrict content or accounts

Beyond specific and notable improvements, most companies lack transparency about how they handle formal government demands and private requests to censor content or restrict accounts.

Ten companies in the RDR Index produce transparency reports containing data about the volume and nature of government demands to remove or restrict online speech. Most of these reports show an increase in government demands over the past two years. For example: **Twitter**'s most recent transparency report, covering government requests to remove content from January to June 2018, found that it had "received roughly 80% more global legal demands impacting approximately more than twice as many accounts, compared to the previous reporting period."[49] **Google**'s most recent transparency report shows that between June 2016 and June 2018, the number of requests received more than tripled.[50] Unfortunately, corporate transparency about the volume and nature of such demands is not improving as demands grow, and, in some cases, transparency is declining.

Figure 11 | How transparent are companies about how they handle government or private requests to censor content or restrict user accounts (F5 - F8)?



While **Facebook** and **Twitter** made significant efforts to disclose more data related to terms of service enforcement as described in the previous section, both actually provided less comprehensive data about government requests to remove, filter, or restrict accounts or content than they did in 2018 (F6). Facebook's transparency report no longer clarified if the data included information about WhatsApp or Messenger, and Twitter no longer included as much detail about requests received related to its video service, Periscope. Facebook's disclosure of its process for responding to third-party requests for content or account restriction (F5) also lacked clarity about what services its process covers. While Twitter's overall score on this indicator improved due to new information that it carries out due diligence and will push back on inappropriate demands, it also failed to clarify whether this policy applied to Periscope as well as its main social networking platform (F5).

On the positive side of the equation: **Apple** published more accessible data about government requests to remove or restrict accounts—which was Apple's only improvement in the Freedom of Expression category. But the company still offered no information about requests to remove content (F6).

How does RDR define government and private requests?

Government requests are defined differently by different companies and legal experts in different countries. For the purposes of the RDR Index methodology, all requests from government ministries or agencies, law enforcement, and court orders in criminal and civil cases, are evaluated as "government requests." Government requests can include requests to remove or restrict content that violates local laws, restrict users' accounts, or to block access to entire websites or platforms. We expect companies to disclose their process for responding to these types of requests (F5), as well as data on the number and types of such requests they receive and with which they comply (F6).

Private requests are considered, for the purposes of the RDR Index methodology, to be requests made by any person or entity through processes that are not under direct governmental or court authority. Private requests can come from a self-regulatory body such as the Internet Watch Foundation, through agreements such as the EU's Code of conduct on countering illegal hate speech online, from individuals requesting to remove or de-list content under the "Right to be Forgotten" ruling, or through a notice-and-takedown system such as the U.S. Digital Millennium Copyright Act (DMCA). We expect companies to disclose their process for responding to these types of requests (F5), as well as data on the number and types of such requests they receive and with which they comply (F7).

See the RDR Index glossary: **rankingdigitalrights.org/2019-indicators/#Glossary**.

Facebook published more accessible data about private requests it received for content or account restrictions (F7). Both Facebook and **Google** improved their policies for notifying users about content or account restrictions: Facebook committed to notify users when the content they created is restricted, and committed to notify users when they try to access content that has been restricted due to a government demand; meanwhile, Google committed to notify Gmail users in certain cases when it restricts access to their account (F8).

Telefónica was more clear than any other telecommunications company about how it responds to government requests to remove, filter, or restrict content or accounts (F5-F7). No telecommunications company revealed any data about requests they received to remove or block content in response to requests that come from entities other than governments, despite the fact that in some countries non-governmental entities, such as the Internet Watch Foundation in the UK, refer websites to telecommunications companies for blocking (F7).[51] Only three telecommunications companies disclosed any data about government requests for content or account restrictions (F6): **AT&T**, **Telefónica**, and **Telenor**. AT&T and Telenor each disclosed the number of requests to block content received per country, whereas Telefónica disclosed more comprehensive information (such as the number of URLs affected and the subject matter associated with the requests), although not consistently for each country in its report.

Some telecommunications companies are starting to disclose more about their user notification policies, with **AT&T**, **Telenor**, and **Telefónica** all disclosing more than others about whether they notify users about blocking content or restricting user accounts (F8). Telenor disclosed that it notifies users when it restricts their account. Telefónica disclosed that it notifies users who attempt to access restricted content that it has been restricted, and the reason for the restriction, when the authorities require them to do so. AT&T disclosed that it attempts to notify users to the extent permitted by law.

4.4 Network management and shutdowns

Users of most internet service providers remain in the dark about why network shutdowns happen or who is responsible.

RDR evaluates whether telecommunications companies clearly explain the circumstances under which they may shut down or restrict access to the network or to specific protocols, services, or applications on the network (F10). Only three companies scored 50 percent or higher on this indicator and only two made any improvements since 2018.

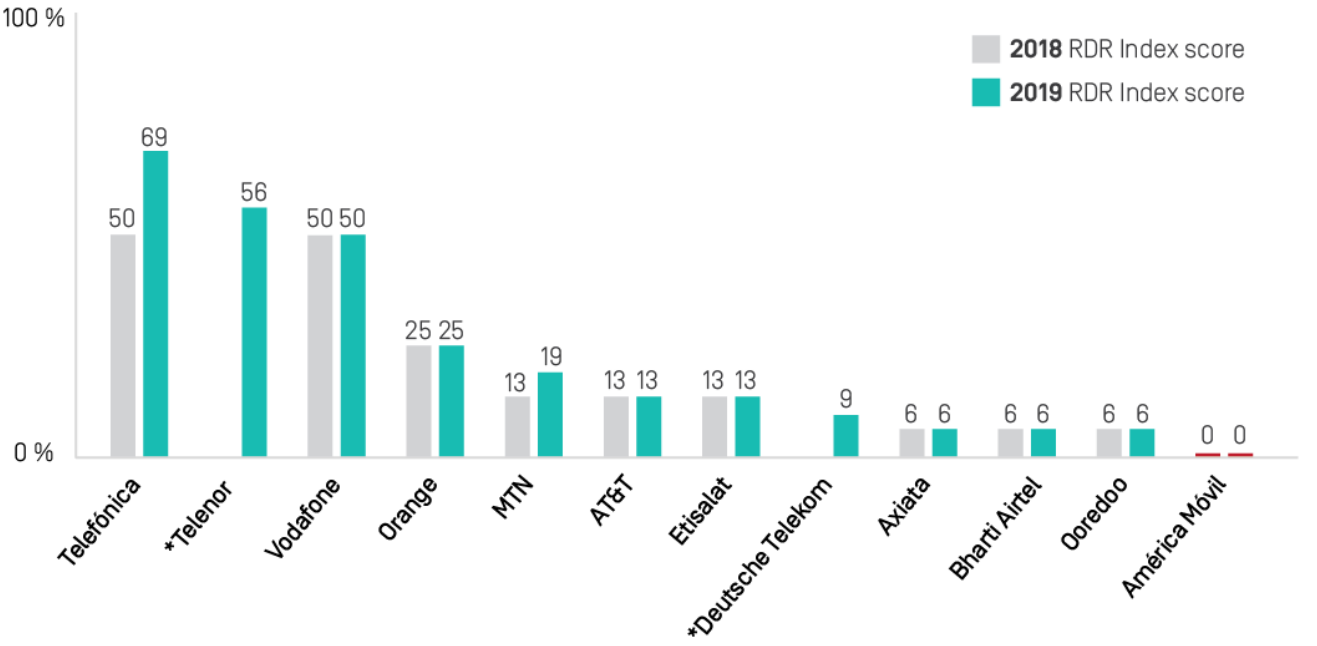
Government network shutdown demands

What the RDR Index evaluates: Indicator F10 evaluates how transparent telecommunications companies are about government demands to shut down or restrict access to the network. It assesses if companies disclose the reasons for shutting down service to an area or group of users, if companies clearly explain the process for responding to government network shutdown requests—including if the company commits to push back on such requests—and if companies disclose the number of these types of requests they receive and comply with.

Read the guidance for Indicator F10 of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#F10**.

An internet shutdown is defined by experts as the "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location often to exert control over the flow of information." According to the Shutdown Tracker Optimization Project run by Access Now, the number of internet shutdowns imposed by governments on internet service providers each year more than doubled between 2016 and 2018.[52]

Figure 12 | How transparent are telecommunications companies about how they handle government demands to shutdown networks (F10)?



**Telenor and Deutsche Telekom were not evaluated in the 2018 RDR Index.*

Putting aside the substantial negative economic implications, the human rights consequences for populations affected by internet shutdowns have been extensively documented. In 2017, the Freedom Online Coalition—a partnership of 30 governments—issued a formal statement expressing "deep concern over the growing trend of intentional state-sponsored disruptions of access to or dissemination of information online. Measures intended to render internet and mobile network services inaccessible or effectively unusable for a specific population or location, and which stifle exercise of the freedoms of expression, association, and peaceful assembly online undermine the many benefits of the use of the internet and ICTs."[53]

Telefónica jumped into first place as the most transparent company about network shutdowns due to improved disclosure of its process for responding to network shutdown demands. It was one of only three companies to disclose any information about the number of shutdown requests it received. It was the only telecommunications company to also disclose the number of requests with which it complied.

Vodafone (unchanged since 2018) and Telenor both disclosed the circumstances under which they may shut down service, and both disclosed a clear commitment to push back on network shutdown demands. Telefónica, Telenor, and Vodafone all clearly disclosed their process for responding to network shutdown demands. **Telefónica** and **Telenor**, a new addition to the RDR Index, both disclosed the number of shutdown demands they

received per country. They also both listed the legal authorities or legal frameworks that can issue shutdown demands or establish the basis for doing so (although they did not list the number of demands per type of authority).

MTN of South Africa was the only other company previously included in the RDR Index to improve its transparency about network shutdowns. It made slight improvements to its disclosure of the reasons why it may shut down its networks, and its process for responding to government shutdown demands.

América Móvil remained the only telecommunications company in the RDR Index to fail to disclose any information about network shutdowns.

Only two companies committed to uphold network neutrality principles and many disclosed little or nothing about their network management policies.

RDR also measures whether telecommunications companies clearly disclose that they do not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network (F9).

Disclosure of network management policies

What the RDR Index evaluates: Indicator F9 assesses how transparent telecommunications companies are about their network management policies and practices. It evaluates if companies publicly commit to upholding net neutrality principles by clearly disclosing that they do not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and network reliability. Companies that offer "zero rating" programs or similar sponsored data programs—or engage in any other types of practices that prioritize or shape network traffic that undermine net neutrality—should not only clearly disclose these practices but should also explain why.

Read the guidance for Indicator F9 of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#F9**.

Telefónica and **Vodafone** distinguished themselves as the most transparent among all telecommunications companies about their network management policies. They were the only two companies in the RDR Index to disclose they do not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network. Five telecommunications companies did not disclose any information about their network management practices: **Deutsche Telekom**, **Etisalat**, **MTN**, **Ooredoo**, and **Orange**.

4.5 Regulatory developments and challenges

In April 2019—less than a month after the massacre of 50 worshippers at two mosques in Christchurch, New Zealand by an Australian white nationalist gunman—the Australian government passed a law imposing steep fines and criminal sentences for company employees if "abhorrent violent material" is not removed "expeditiously." Australian media companies and human rights groups vigorously opposed the law, warning that it would lead to censorship of journalism and activism. Yet it was passed without meaningful public consultation or any form of impact assessment.[54]

It has long been standard practice of authoritarian governments to hold internet services and platforms strictly liable for users' speech, with government authorities defining terrorism and disinformation so broadly that companies are forced to proactively censor speech that should be protected under human rights law.[55] Faced with problems of terrorist incitement and deadly hate speech propagated through internet platforms and services, a number of democracies are also moving to increase the legal liability of companies that fail to delete content transmitted or published by users. The box below lists recent laws affecting freedom of expression in home markets of many companies included in the RDR Index.

Regulations affecting freedom of expression proposed or enacted since 2018

The following is a (non-exhaustive) list of proposed or enacted legislation in 2018 and 2019 in regions or countries where the companies we evaluate are headquartered.

The European Union: In April 2019, the European Parliament approved the Regulation on Tackling the Dissemination of Terrorist Content Online, requiring platforms to remove certain content within an hour of notification or face fines of up to 4 percent of a company's annual global turnover.[56] The regulation will be further negotiated before being finalized. The EU passed the Directive on Copyright in the Digital Single Market, which was heavily contested by digital rights activists for including measures critics say could undermine freedom of expression and lead to over censoring content.[57]

France: In December 2018, France enacted a new misinformation law.[58] Designed to impose strict rules on the media during the three months preceding any election, the law targets "fake news" that seeks to influence electoral outcomes. The law includes a "duty of cooperation" for online platforms.

Germany: In January 2018, the Network Enforcement Act (NetzDG) went into effect.[59] It targets the dissemination of hate speech and other illegal content online by requiring social networks to remove content within 7 days—and in some cases within just 24 hours—or face hefty fines.

The United Kingdom: In April 2019, the UK government published an Online Harms White Paper which proposes making internet companies responsible for illegal, harmful, or disreputable content on their platforms and introducing a new regulator with enforcement authority.[60] It includes a proposal that company executives be held personally liable for harmful content appearing on their platforms.

China: In November 2018, China released the Regulation on Security Assessment of Internet Information Services Having Public-Opinion Attributes or Social Mobilization Capabilities.[61] It obliges companies to monitor—and in some instances block—signs of activism or opinions deemed threatening by the government.

India: In December 2018, India published the Information Technology [Intermediary Guidelines (Amendment) Rules].[62] Under the draft rules, officials could demand social media companies to remove certain posts or videos. Though the rules clarify that requests must be issued through a government or court order they also require service providers to proactively filter unlawful content. Critics say the types of content that service providers would be required to prohibit go beyond constitutional limitations on freedom of expression.

Russia: In March 2019, Russia passed two laws that make it a crime for individuals and online media to "disrespect" the state and spread "fake news" online, authorizing the government to block websites, impose fines, and jail repeat offenders.[63] In May 2019, Putin signed the controversial “Sovereign Internet” legislation, which will further solidify the government’s control over the internet.

A key human rights concern is that intermediary liability can be abused, particularly when definitions of disinformation, hate speech, and extremism are subject to debate even in some of the world’s oldest democracies.[64] Another concern stems from evidence gathered by researchers in countries where strict liability laws are already in force: when in doubt platforms can be expected to over-censor if they face steep fines or other penalties for under-censoring.[65] Such “collateral censorship” can silence journalism, advocacy, and political speech when companies’ automated mechanisms—and even human moderators operating under extreme time pressure without sufficient understanding of cultural contexts and local dialects or slang—are often not capable of telling the difference between journalism, activism, satire, or debate on the one hand, and hate speech or extremism on the other.[66]

Certainly, companies need to be able to recognize and react quickly to urgent life-and-death situations, such as the Christchurch shooting or the Myanmar genocide in 2017,

during which hate speech in support of ethnic purges was disseminated via Facebook.[67] But given the human rights risks associated with increased intermediary liability for users' speech and behavior, some legal experts suggest shifting the regulatory focus away from liability and instead require companies to take broader responsibility for their impact on society, and to build businesses committed to treating users fairly and humanely.[68]

David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, calls on governments to focus on "ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums."[69] Terms of service should be based on human rights standards, developed and constantly improved upon through a process of public consultation, risk assessment, and external review. To guard against abuse of regulations related to online speech, Kaye also emphasizes that judicial authorities—not government agencies—should be the arbiters of what should be considered lawful or illegal expression. Furthermore, governments should release their own data to the public about all demands made of companies to restrict speech or access to services, subject themselves to oversight mechanisms in order to prevent abuse, and ensure that the law imposes appropriate legal penalties upon officials or government entities who abuse their power.

Developing effective capabilities to stop serious harms without inflicting collateral damage on the legitimate rights of others will require greater collaboration between governments, companies, and civil society than has yet occurred. Innovation is needed in technical design, business practices, and government regulatory approaches, in addition to more active engagement with civil society and subject-matter experts as part of the risk assessment and mitigation process. Special attention must be paid to politically sensitive regions, ethnic conflicts, and civil wars in addition to elections.

A clear first step is not merely to encourage, but to require companies to improve their governance, oversight, and due diligence to mitigate and prevent their products, platforms, and services from corroding human rights of users and the communities in which they live. As discussed in Chapter 3, regulations requiring strong corporate governance and oversight of human rights risks are badly underdeveloped.

Secondly, companies committed to respecting freedom of expression must maximize transparency about all the ways that content and information flows are being restricted or otherwise manipulated on their platforms and services. This is especially vital at a time when government demands, mechanisms, and regulatory frameworks are evolving rapidly and unpredictably in scope and scale around the world.

As the 2019 RDR Index results clearly show, companies have not come close to the maximum degree of transparency about all the ways that freedom of expression can be constrained via their platforms and services. In the current regulatory climate, greater transparency could hardly be more urgent.

4.6 Recommendations for companies

1. Commit to robust governance: Board-level oversight, risk assessment, stakeholder engagement, and strong grievance and remedy mechanisms are all essential for mitigating risks and harms before the problems become so severe that governments are compelled to step in and regulate. (See also the governance recommendations in Chapter 3.)

2. Maximize transparency: Companies should publish regular transparency reports covering actions taken in response to external requests as well as proactive terms of service enforcement. Such reports should include data about the volume and nature of content that is restricted, blocked, or removed, or information about network shutdowns, as well as the number of requests that were made by different types of government or private entities.

3. Provide meaningful notice: In keeping with the Santa Clara Principles for content moderation and terms of service enforcement (santaclaraprinciples.org), companies should give notice to every user whose content is taken down or account suspended, explain the rationale or authority for the action, and provide meaningful opportunity for timely appeal. (See also the remedy recommendation in Chapter 3.)

4. Monitor and report on effectiveness of content-related processes: Companies should monitor and publicly report on the quantitative and qualitative impact of their compliance with content removal regulations, in order to help the public and government authorities understand whether existing regulations are successful in achieving their stated public interest purpose. Conduct and publish assessments on the accuracy and impact of removal decisions made by the company when enforcing its terms of service, as well as actions taken in response to regulations or official requests made by authorities, including data about the number of cases that had to be corrected or reversed in response to user grievances or appeals.

5. Engage with stakeholders: Maximize engagement with individuals and communities at greatest risk of censorship and who are historically known to have been targets of persecution in their societies, as well as those most at risk of harm from hate speech and other malicious speech. Work with them to develop terms of service and enforcement mechanisms that maximize the protection and respect of all users' rights.

4.7 Recommendations for governments

1. Require strong corporate governance and oversight: Specifically, require companies to publish information about their human rights risks, including those related to freedom of expression and privacy, implement proactive and comprehensive impact assessments, and establish effective grievance and remedy mechanisms. (See also the recommendations for governments in Chapter 3.)

2. Require corporate transparency: Companies should be required to include information about policies for policing speech, as well as data about the volume and nature of content that is restricted or removed, or accounts deactivated for any reason.

3. Be transparent: Governments should publish accessible information and relevant data about all requirements and demands made by government entities (national, regional, and local) that result in the restriction of speech, access to information, or access to service. For governments that are members of the Open Government Partnership—an organization dedicated to making governments more open, accountable, and responsive to citizens—transparency about requests and demands made to companies affecting freedom of expression should be considered a fundamental part of that commitment.

4. Assess human rights impact of laws: While requiring companies to conduct assessments, governments should also be required by law to conduct human rights impact assessments on proposed regulation of online speech. Any liability imposed on companies for third-party content should be consistent with international human rights instruments and other international frameworks, as outlined by the Manila Principles on Intermediary Liability (manilaprinciples.org).

5. Ensure adequate recourse: Governments should ensure that individuals have a clear right to legal recourse when their freedom of expression rights are violated by any government authority, corporate entity, or company complying with a government demand.

6. Ensure effective and independent oversight. Any government bodies empowered to flag content for removal by companies, or empowered to require the blockage of services, or to compel network shutdowns, must be subject to robust, independent oversight and accountability mechanisms to ensure that government power to compel companies to restrict online speech, suspend accounts, or shut down networks is not abused in a manner that violates human rights.

7. Collaborate globally: Governments that are committed to protecting freedom of expression online should work proactively and collaboratively with one another, as well as with civil society and the private sector, to establish a positive roadmap for addressing online harms without causing collateral infringement of human rights.

5. Privacy

Data privacy has become a key issue over the past several years, with both lawmakers and the public crying foul over the lack of accountability and transparency by companies about how they handle user data.

As news about privacy breaches and deceptive practices involving major U.S.-based companies continued to dominate headlines over the past year, tough new data protection regulations came into force in Europe and in a number of countries around the world. Regulatory efforts and debates in the U.S. gained new urgency, as it became clear that the U.S. cannot afford to remain so far out of step with major global trends on privacy regulation. The state of California—unwilling to wait for national action—passed its own privacy law. Even companies that had previously lobbied against comprehensive national privacy regulation in the U.S. have embraced the inevitable and expressed support for regulation, hoping to be able to influence its final shape.

Nearly all ranked companies made some improvements to their disclosures of policies and practices related to privacy in the past year. However, companies that led the Privacy category of the 2019 RDR Index distinguished themselves by going beyond minimum legal requirements—at least in certain areas, even if they were deficient in others. This demonstrates that current data protection regulations alone may not be sufficient to hold companies accountable for the broader spectrum of policies affecting users' privacy. Regulations also need to address issues like data security as well as how companies allow third parties, like advertisers or governments, access to user data. Results from this year's Index show that while many companies made concrete improvements in areas that appear to be largely driven by regulatory demands, there remains ample room for improvement. (For a discussion of regulatory trends and gaps, see section 5.6.).

5.1 Transparency remains inadequate

Most companies still do not disclose enough about policies and practices affecting users' privacy.

How much do we really know about what data companies collect, hold, and share—with other companies, with advertisers, or with government authorities including law enforcement? How much control do people really have over what is collected and shared about them, and with whom? How much do we know about what companies are doing to keep our data secure?

As in previous years, the answer to these questions is: *not enough*. Despite some positive steps forward, results from the 2019 RDR Index show that most of the 24 companies evaluated failed to meet minimum standards of transparency about how they handle and secure users' data.

While nearly all companies in the 2019 RDR Index made some improvements over the last year, no company scored higher than 60 percent in the Privacy category—and most earned a score of just 50 percent or lower (see Figure 13 below). This means no company in the RDR Index disclosed enough about their policies and practices for their users to fully understand the full range of privacy and security risks they face when using their services.

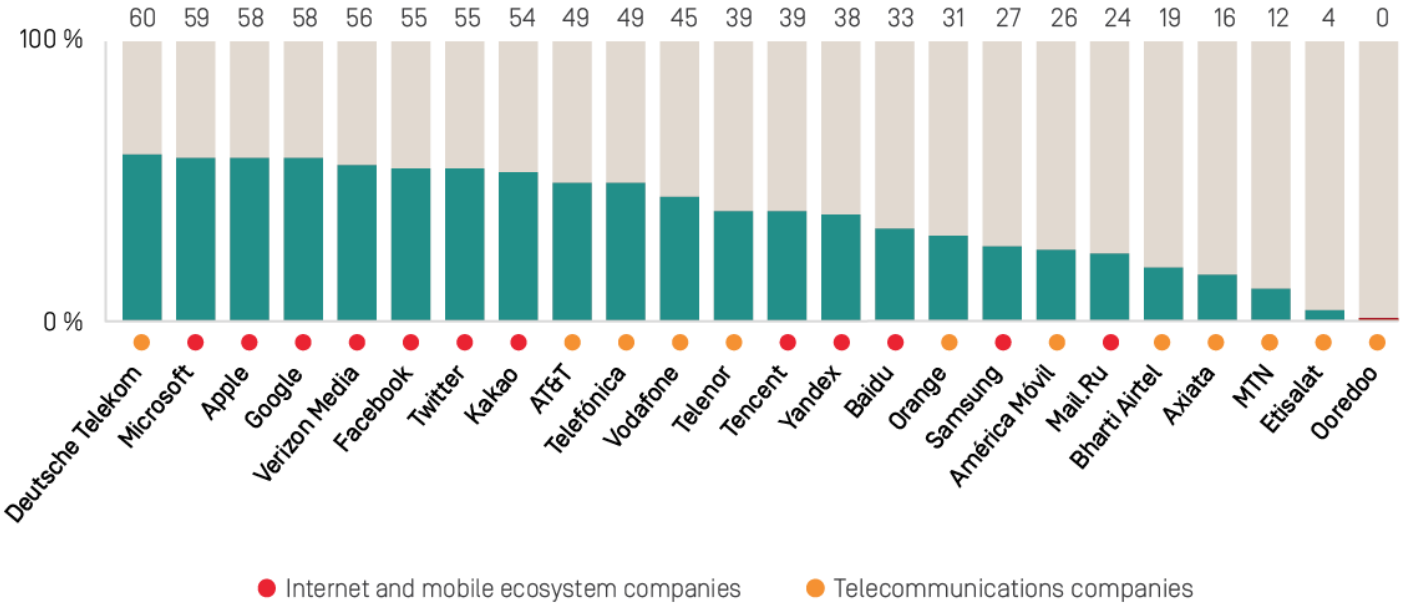
How transparent are companies about policies and practices affecting privacy?

What the RDR Index evaluates: The RDR Index evaluates company disclosure of policies and practices affecting privacy across 18 indicators that collectively address how transparent companies are about what they do with user information, with whom they share it, and what they do to secure it.[70] Indicators assess:

- **Accessibility and clarity of privacy policies:** How clear and accessible companies make their privacy policies, and if and how they notify users when they make changes to these terms (P1, P2).
- **User information:** How transparent companies are about how they collect, share, and handle user information (P3-P9).
- **Government demands:** How companies handle government and other types of third-party requests for user information (P10, P11, P12).
- **Security:** If companies have clear processes and safeguards in place for keeping user information secure (P13-P18).

To review the privacy indicators of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#P.**

Figure 13 | How transparent are companies about policies and practices affecting users' privacy and security (P1-P18)?



As Figure 13 above shows, German telecommunications company **Deutsche Telekom** earned the highest average privacy score of all companies—including internet and mobile ecosystem companies. This is the first time since publishing our inaugural ranking in 2015 that a telecommunications company topped the Privacy category.[71] The company's high score on privacy-related policies and disclosures was due to its stronger disclosure of its handling of user data, and of its security policies, relative to its peers.

Telecommunications companies across the board disclosed little or nothing about their relationships with governments—how they handle demands by government entities or law enforcement to hand over user data. In many cases this gap in disclosure explains their low scores in the Privacy category in relation to internet and mobile ecosystem companies. Apart from **Deutsche Telekom**, most telecommunications companies also did not disclose enough about how they handle user information, and were particularly opaque about their data retention policies and practices. Notably, two telecommunications companies—Qatar-based **Ooredoo** and UAE-based **Etisalat**—failed to publish privacy policies at all.

Among internet and mobile ecosystem companies, **Microsoft** earned the highest average score in the Privacy category for its stronger disclosure of its handling of government requests for user information, and of its security policies. The company made notable improvements to its disclosure of its data breach policies (P15), and rolled out an end-to-end encryption option for both Outlook and Skype (P16).

Apple and **Google** tied for the second-best score on privacy-related disclosures among internet and mobile ecosystem companies, after **Microsoft**. Apple disclosed more about its security policies than any other internet and mobile ecosystem company, and stood out for having the strongest disclosure of encryption policies and practices of all of its peers. Google's high score was due to stronger disclosure of how it handles government requests for user information. Apart from **Twitter**, it also disclosed more about how it handles user information than all other internet and mobile ecosystem companies evaluated—although there is ample room for improvement.

Although **Facebook** and **Twitter** made key improvements, both companies earned a score of just 55 percent, tying for fifth in the Privacy category among internet and mobile ecosystem companies. Twitter disclosed more than all other internet and mobile ecosystem companies about its handling of user information, but received one of the lowest scores among its peers on indicators evaluating disclosure of security policies (P13-P18); the company failed to reveal anything at all about what policies it has in place to respond to data breaches (P15).

Facebook made notable improvements to its disclosure about how it handles user information, but still did not give users a clear picture of what it does with user data, nor did it provide users with clear options to control what data is shared. The company also disclosed insufficient information about its security policies, including safeguards around employee access to user data and its policies for handling data breaches.

Chinese internet companies **Baidu** and **Tencent** also made significant improvements to their privacy and security disclosures, which may be a result of new directives that came into effect in May 2018 requiring companies to be more transparent about different aspects of how they handle personal data.[72]

5.2 Handling of user information

New data protection regulations in the EU and elsewhere seem to be pushing companies in the right direction—but critical gaps need to be addressed if companies are to be fully accountable about how personal data is handled.

Nearly every company evaluated in this year's RDR Index updated their privacy policies in 2018, as new data protection regulations came into effect in the EU as well as in several countries around the world. But what does this mean for users? Do people know more about what their mobile phone service or internet platform is doing with their data than they did a year ago? Do people have more control over what data about them is being collected and shared, and with whom? (For more about data protection regulations that same into force in 2018, see section 5.6.)

How transparent are companies about their handling of user information?

What the RDR Index evaluates: The RDR Index has seven indicators evaluating how transparent companies are about how they handle user information.[73] We expect companies to disclose: each type of user information they collect (P3); each type of user information they share, including the types and names of the third parties with whom they share it (P4); the purpose for collecting and sharing user information (P5); and their data retention policies, as well as time frames for storage and deletion (P6).

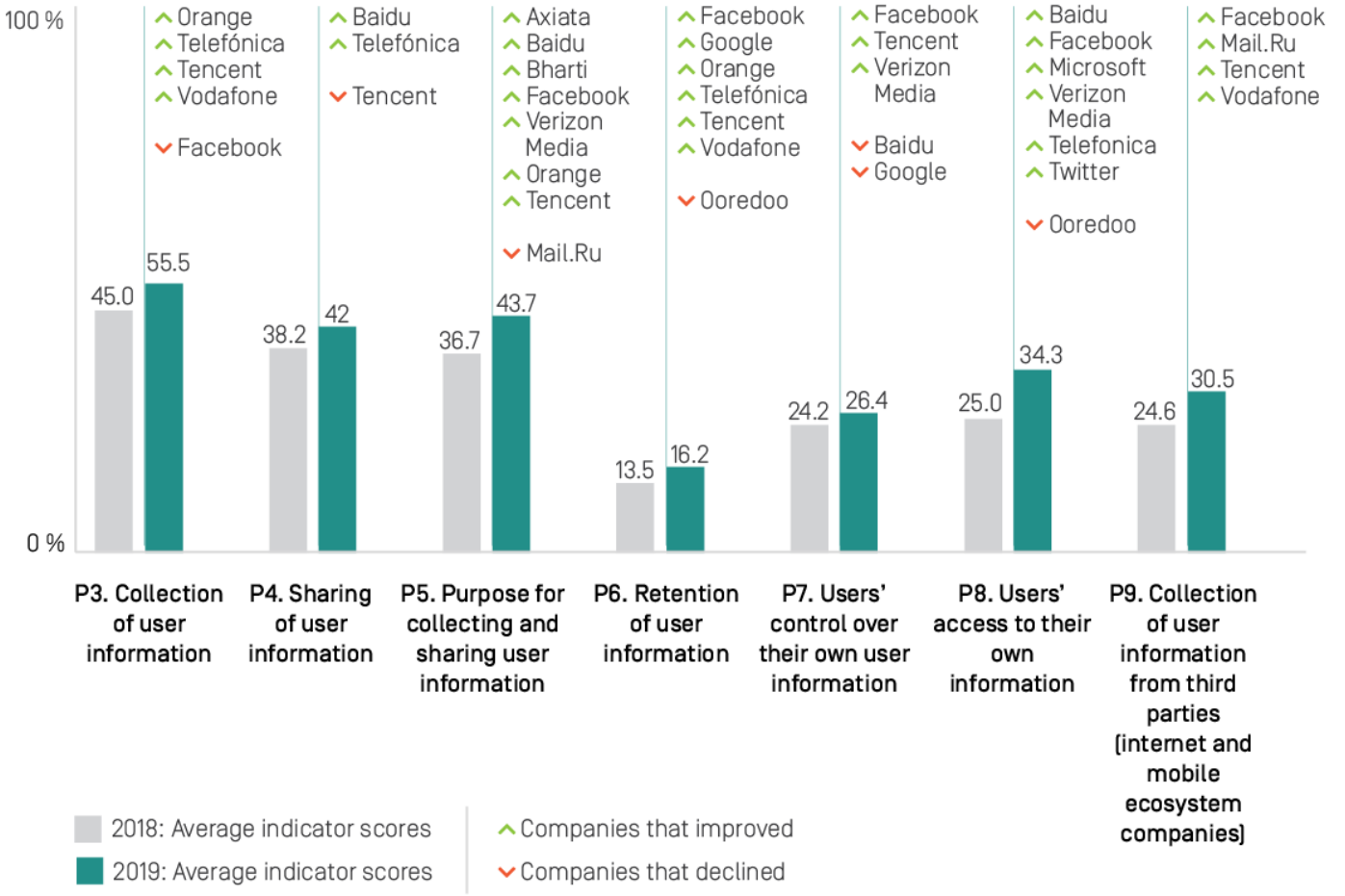
Companies should also disclose options users have to control what information is collected and shared, including for the purposes of targeted advertising (P7), and should clearly disclose if and how they track people across the internet using cookies, widgets, or other tracking tools embedded on third-party websites (P9). We also expect companies to clearly disclose if and how users can obtain all public-facing and internal data companies hold about users, including metadata (P8).

User information: RDR defines "user information" 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. User information is any data that documents a user's characteristics and or activities—which may or may not be tied to a specific user account—and 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.

See the privacy indicators of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#P**.

Results were mixed. Figure 14 below shows improvements and declines by companies across all indicators evaluating disclosure of how they handle user information. A majority of companies—13 of the 22 companies evaluated in the 2018 RDR Index—made some improvements by clarifying different aspects of how they handle user information. But there were also key areas where companies made little progress—or in some cases, disclosed even less about their handling of user data than they had previously.

Figure 14 | How have companies improved their disclosure of how they handle user information (P3-P9)?



Notable trends include:

Improved clarity about reasons for collecting and sharing user data (P5). Seven companies—**Axiata**, **Baidu**, **Bharti Airtel**, **Facebook**, **Orange**, **Tencent**, and **Verizon Media**—improved their transparency about why they collect and share user data although, on average, the scores for this indicator remained low. Notably, the Chinese internet company Baidu earned the highest score on this indicator due to its improved disclosure about its purpose for sharing user information, and for clearly committing to limit its use of data to the purpose for which it was collected. But the Russian internet company **Mail.Ru** lost points on this indicator: its revised privacy policy for the social network VKontakte no longer mentioned a commitment to limit its use of data to the purpose for which it was collected, which was disclosed in the previous version, evaluated for the 2018 RDR Index.

Improved options for users to obtain their data (P8)**.** Six companies—**Baidu**, **Facebook**, **Microsoft**, **Telefónica**, **Twitter**, and **Verizon Media**—clarified how people can obtain the data that these companies hold about them. Facebook this year earned the highest score on this indicator, after clarifying options users have to obtain their data for all of Facebook's services, including the Facebook social network service, WhatsApp, and Instagram.

Improved clarity about data retention (P6). Six companies—**Facebook**, **Google**, **Orange**, **Telefónica**, **Tencent**, and **Vodafone**—improved their disclosure of their data retention policies. However, most companies were the least transparent about these policies than about any other aspects of how they handle user information.

Improved clarity of what data is collected (P3). Four companies—**Orange**, **Telefónica**, **Tencent**, and **Vodafone**—improved their disclosure of what types of data they collect. Tencent disclosed more than any other company in the RDR Index about what types of data it collects and how it collects it. **Facebook** lost points on this indicator for disclosing less clear information about how Instagram collects user information.

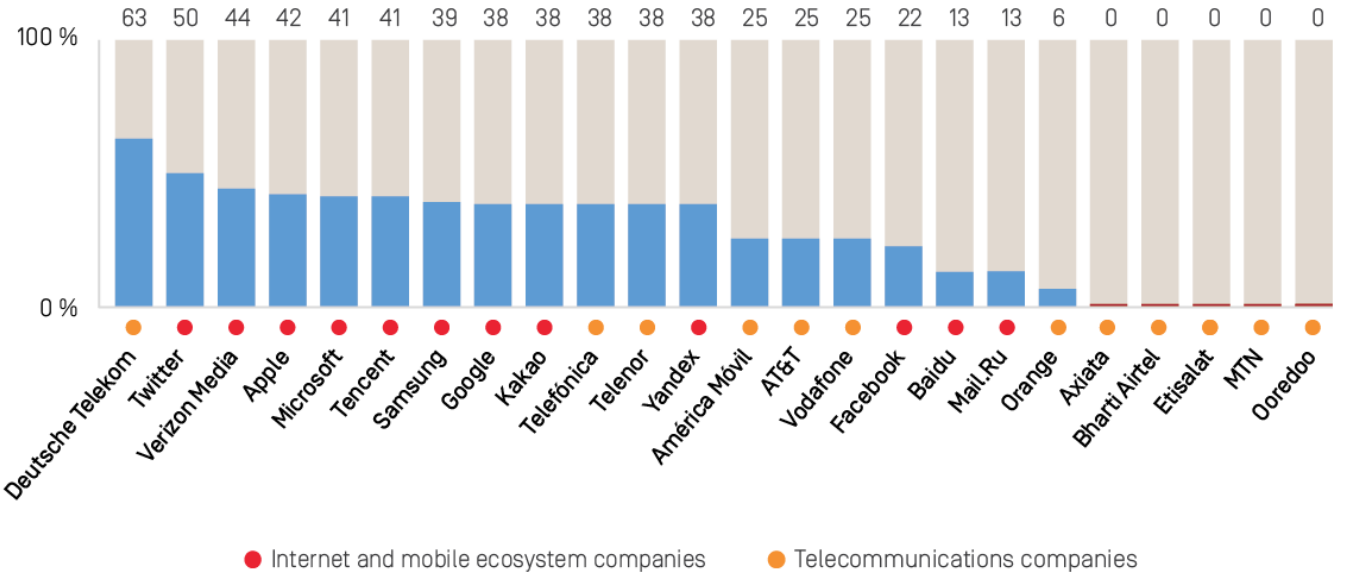
5.3 Privacy gaps: Collection and sharing

Despite improvements, companies still don't give users enough control over what data is collected and shared.

Indicator P7 evaluates if companies give users clear options to control what information is collected and shared about them, including for the purposes of targeted advertising.[74] We expect companies to clearly disclose options for users to control what information is collected about them, and to delete specific types of information without requiring users to delete their entire account. We also expect companies to give users options to control how their information is used for advertising and to disclose that targeted advertising is *off* by default.

The 2018 RDR Index showed that most companies gave unclear options for users to control what is collected and shared about them, and how that data is used for the purposes of targeted advertising.[75] Results of the 2019 RDR Index show that companies made little progress in this area. Just three companies—**Facebook**, **Tencent**, and **Verizon Media**—improved their disclosure of options users have to control what information is collected and shared about them.

Figure 15 | How transparent are companies about options users have to control their own information (P7)?



Deutsche Telekom was the most transparent of all companies about giving users options to control what information is collected and shared about them, including for the purposes of targeted advertising. In addition to disclosing user options to control what information is collected, and to delete some of this data, Deutsche Telekom was the only company evaluated in the RDR Index to disclose that targeted advertising is off by default: users must opt-in in order for their data to be used for this purpose—and they can revoke their consent at any time.

Yet the other European telecommunications companies in the RDR Index—**Orange**, **Telefónica**, **Telenor**, and **Vodafone**—disclosed notably little about what options people have to control how companies use their data. Orange disclosed far less than its peers: it lacked clarity about what options users have to control what types of data it collects. Nor did it clearly specify what types of data can be deleted. It also disclosed very limited options for users to control if and how their data is used for the purposes of targeted advertising and did not indicate if targeted advertising was off by default.

Among internet and mobile ecosystem companies, **Twitter** disclosed more than any of its peers about options users have to control what data is collected and shared. It was one of the few companies to disclose options for users to control how their data is used for targeted advertising.

Google lost points on this indicator this year after revising its disclosure about whether Android users can turn off their location data. The company previously stated that

Android users could control whether the company collected location data through a setting at the device level. However, Google's revised policy on managing location history stated that some location data may still be collected even when location history is turned off.

Facebook disclosed slightly more than in the previous year about ways users can control their information—it provided two examples of types of data that users can delete—but it remained one of the lowest-scoring companies on this indicator (although up from having the very lowest score on this indicator in the 2018 RDR Index).

Few companies disclosed enough about their data retention policies for users to give informed consent about what companies are doing with their data.

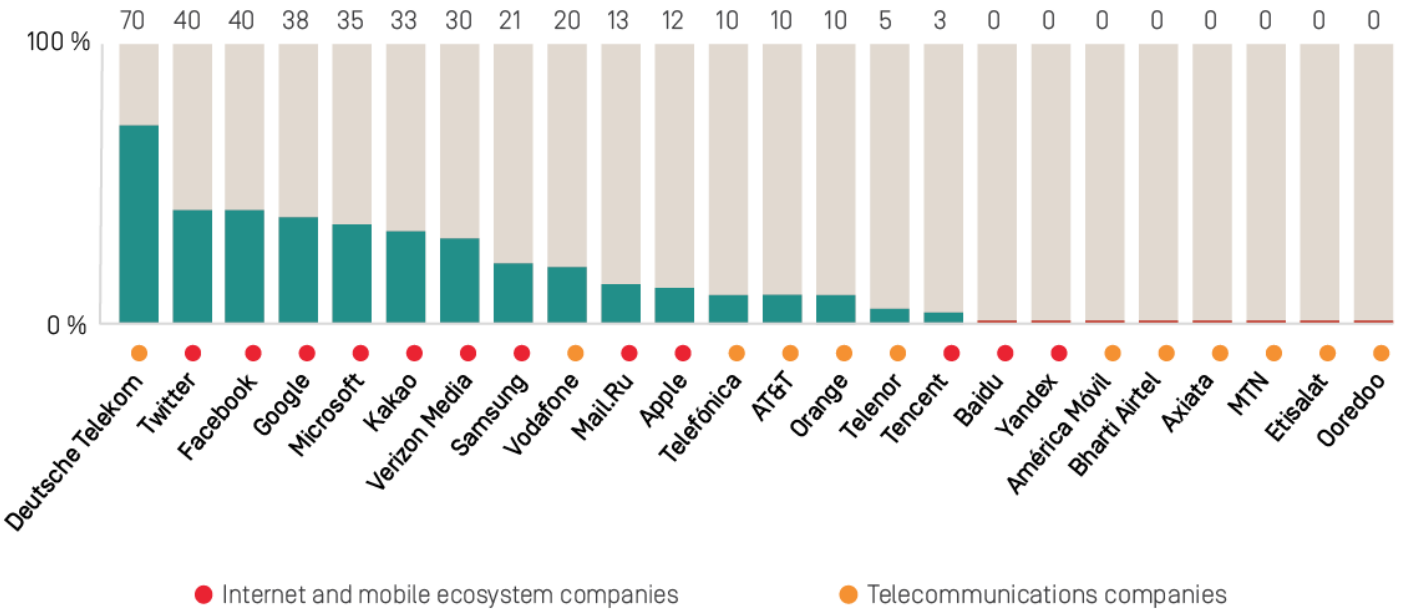
Indicator P6 evaluates how transparent companies are about their data retention policies. The RDR Index expects each company to clearly disclose how long they retain each type of user data they collect, including what de-identified data they retain—as well as its process for de-identifying that data—and its time frames for deleting user data after a user's account is terminated.

RDR defines "de-identified" user information as data that companies collect and retain but only after removing or obscuring any identifiable information from it. This includes explicit identifiers like names, email addresses, and any government-issued ID numbers, as well as identifiers like IP addresses, cookies, and unique device numbers.

See the RDR Index glossary of terms at:
rankingdigitalrights.org/2019-indicators.

As with other indicators in the RDR Index evaluating disclosure of data handling policies, **Deutsche Telekom** earned the top score on Indicator P6, disclosing more about its data retention policies than any other company evaluated. The company provided time frames for retaining some types of user data it collects, and revealed more about what de-identified user data it retains than any of its peers.

Figure 16 | How transparent are companies about their data retention policies and practices (P6)?



As Figure 16 above shows, half of the 12 telecommunications companies evaluated in the 2019 RDR Index received no points on Indicator P6 because they provided no information about any aspect of their data retention policies evaluated in this indicator. Among European telecommunications companies, **Telefónica**, **Telenor**, and **Vodafone** each disclosed some information about how long they retain user data, but revealed nothing further about policies for de-identifying user information, or if they delete all user information after the account is terminated. Notably, although **Orange** improved its disclosure by providing a time frame for deleting some types of data after users terminate their account, it still earned one of the lowest scores among telecommunications companies on this indicator.

Among internet and mobile ecosystem companies, **Twitter** tied with **Facebook** for the top score on this indicator (P6)—although a high score of just 40 percent on this indicator reflects how little companies disclosed about their data retention policies. Twitter revealed how long it retains some of the user information it collects, and disclosed what de-identified data it retains, and its process for de-identifying some of that data. Facebook earned a score improvement by providing examples of retention periods for certain types of user information for Facebook, Instagram, and Messenger, and by committing to delete some types of user information after users terminate their Instagram accounts.

Notably, **Apple** was among the least transparent internet and mobile ecosystem companies, apart from Chinese companies **Tencent** and **Baidu**, about its data retention

policies. It received a small amount of credit on this indicator for disclosing that it retains location data in a de-identified format, but did not disclose if it does so for other personally identifying data, like IP addresses. It also disclosed nothing about time frames for storing any of the data it collects or when it deletes data after users terminate their accounts.

5.4 Government demands

No company disclosed enough about how they handle government demands to hand over user data, which could expose users to a range of unknown privacy and security risks.

As people depend more on internet and mobile technologies to carry out their daily activities, the data that companies collect about us—tracking our movements, our communications, our web searches, and more—has become a key target for governments and law enforcement. Companies are often caught in the middle between keeping users' information secure and private, and complying with government demands. Their choices can have dire consequences—particularly when complying with requests from authoritarian regimes where rule of law is weak.

In addition, the rise in anti-terrorism laws around the world—in democratic and authoritarian countries alike—have put increasing pressure on internet and telecommunications companies to provide authorities with access to user data. In its latest *Freedom on the Net* report, Freedom House documented a substantial increase in laws around the world related to government surveillance in the past two years alone: "Governments in 18 out of 65 countries have passed new laws or directives to increase state surveillance since June 2017, often eschewing independent oversight and exposing individuals to persecution or other dangers in order to gain unfettered access."[76] These laws can include requirements for companies to store data locally and for longer periods of time, lowered legal barriers for authorities to demand that companies hand over data, or regulations aimed at circumventing encryption, all of which can increase the likelihood that a user's sensitive information ends up in the hands of the government.

In an era of pervasive state surveillance, companies need to be fully transparent about their relationships with governments, including with law enforcement, so that people can make informed choices about if and how to use a particular company's platform or service. Companies should disclose how they handle government demands to hand over user data—and commit to push back on overly broad demands and demands that are not consistent with governing legal frameworks—and publish data about the number and type of requests for user data they receive and comply with. They should also be clear about whether they inform users when their data has been requested by law enforcement—or cite the legal reason prohibiting them from doing so.

What does RDR mean by "government demands"?

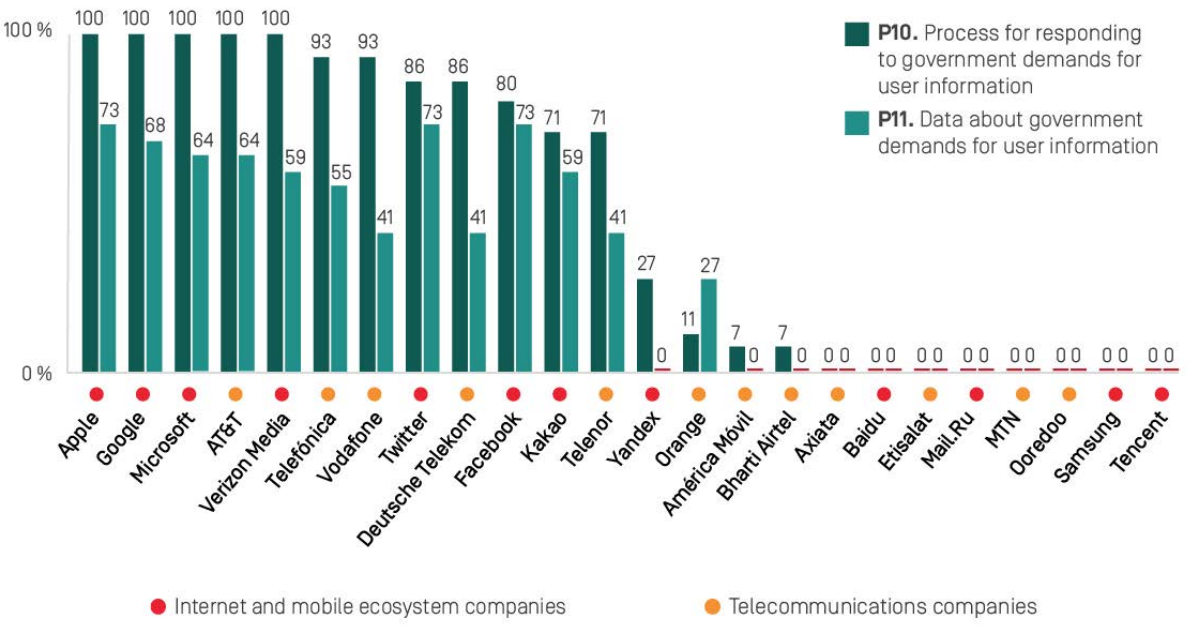
Companies receive a growing number of requests from governments to turn over user information. These requests can come from government ministries or agencies (including from foreign jurisdictions), law enforcement, and court orders in criminal and civil cases, and include requests for real-time access and stored information.

What the RDR Index evaluates: We expect companies to publicly disclose their process for responding to each type of government request they receive—whether through courts, law enforcement, or foreign jurisdictions—along with the basis for complying with these demands. Companies should also publicly commit to pushing back on inappropriate or overbroad requests, to notify users of requests for their information to the extent legally possible, and to disclose the types of cases in which they would be legally prohibited from providing notification. We also expect companies to regularly publish data about the number of government requests they have received and with which they have complied, including the type of government authority that issued the request, whether the demand sought communications content or non-content or both, and whether there are some types of requests about which it is legally prohibited from disclosing specific data.

See the privacy indicators of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#P**.

As in previous years, results from the 2019 RDR Index show that internet and mobile ecosystem companies disclosed more than telecommunications companies about their processes for handling government demands, and published more data about their compliance with these requests (see Figure 17 below).

Figure 17 | How transparent are companies about how they handle government demands for user information (P10, P11)?



Scores here are calculated from elements in Indicators P10 and P11 evaluating company disclosure of their handling of government demands.

Notably, a handful of U.S.-based companies—**Apple**, **Google**, **Microsoft**, **Verizon Media**, and **AT&T**—all earned full credit for comprehensive disclosure of their processes for handling government requests, including those from foreign jurisdictions, and for publishing a clear commitment to push back on overly broad requests (P10). But these companies were less transparent about the actions they took as a result of these demands (P11), due at least in part to legal restrictions: U.S. law prohibits companies from disclosing exact numbers of government requests received for stored and real-time user information under Foreign Intelligence Surveillance Act (FISA) requests or National Security Letters (NSLs), which prevented U.S. companies from being fully transparent in this area.[77] As in the 2018 RDR Index, Verizon Media disclosed less data than all other U.S. internet and mobile ecosystem companies about government demands for user information.

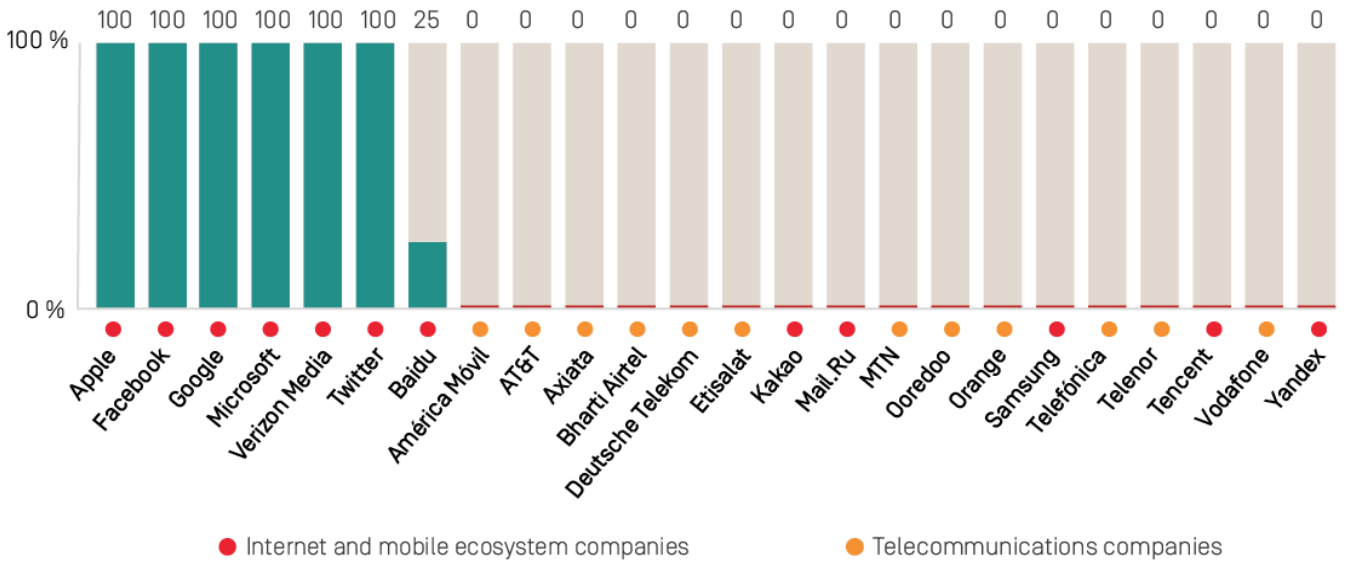
Despite falling short in some other privacy areas, high scores on indicators evaluating transparency of handling government demands explains why U.S. internet and mobile ecosystem companies like **Google** and **Facebook** earned higher scores in the Privacy category than most of the European telecommunications companies. The European telecommunications companies evaluated, especially those that are members of the Global Network Initiative (GNI), have over the last few years begun to take concrete steps to improve their transparency around their processes for handling government demands. **Telefónica** and **Vodafone** in particular have started to publish more robust and comprehensive reports explaining their processes for handling these types of demands across their global operations. Telefónica improved this year by giving more detailed information about the company's process for responding to government requests.

While these are positive steps forward, European telecommunications companies still did not disclose enough actual data detailing the number and types of these requests they received and complied with, either in their home markets or across the various markets in which they operate (P11). **Orange**, notably, was the least transparent of all of its European peers: It revealed the legal basis for complying with the French government's requests, but gave no information about how it responds to these requests or those submitted by foreign governments to its operating companies in other jurisdictions (P10). It published some data about its compliance with government requests in France but not about its handling of requests in other countries where it operates (P11).

The biggest gap in disclosure between internet and mobile ecosystem companies and telecommunications companies was around user notification policies. Indicator P12 of the RDR Index asks if companies clearly disclose if they notify users when government entities, including courts or other judicial bodies, request their data. It also asks companies to disclose circumstances when they might *not* notify users, and to explain the types of government requests they are legally prohibited from disclosing.

As Figure 18 below shows, all U.S.-based internet and mobile ecosystem companies—**Apple**, **Google**, **Microsoft**, **Verizon Media**, **Twitter**, and **Facebook**—published a clear commitment to notify users when governmental entities request their data, and offered clear explanations about when they might not notify them, including the types of government requests they are prohibited by law from disclosing.

Figure 18 | Do companies commit to notify users when governments request their data (P12)?



Scores calculated from Elements 1 and 3 of Indicator P12. View elements and P12 data at: www.rankingdigitalrights.org/index2019/indicators/p12/

Notably, Chinese internet company **Baidu** earned some credit on this indicator this year for disclosing that it may hand over user data to officials or courts without notifying users in cases of national security or criminal proceedings.

However, no telecommunications company in the entire RDR Index scored any points on this indicator (P12)—meaning that not one of the 12 telecommunications companies evaluated by the RDR Index publicly committed to notifying users when governments request their data, nor did any of these companies provide a legal reason for not doing so. This means that people who use the internet and mobile phone services provided by these companies have no idea if governments or law enforcement are surveilling or otherwise accessing their communications, whether lawfully or not.

5.5 Security trends

Despite some improvements, most companies do not disclose enough about their security policies for users to be able to make informed choices.

Data security is central to people's privacy. Security breaches can expose personal and financial information, which comes with a range of short- and long-term privacy risks. But for members of vulnerable communities—including journalists, activists, and members of minority groups—data security can also have physical safety implications. It is incumbent on companies to ensure that the user data they collect and share is strictly secured and, when compromised, to swiftly inform users.

The RDR Index has six indicators evaluating company disclosure of security policies and practices (P13-P18). We do not expect companies to divulge a level of detail about their security procedures that could compromise their security systems or expose them to attack. But we do expect companies to disclose basic information affirming that they follow industry best practices around security so that users can understand what the possible risks are and can make informed decisions about if and how to use a company's services.

How transparent are companies about their policies and practices for keeping user information secure?

What the RDR Index evaluates: The RDR Index contains six indicators evaluating company disclosure about their policies and practices for keeping user data secure. These evaluate:

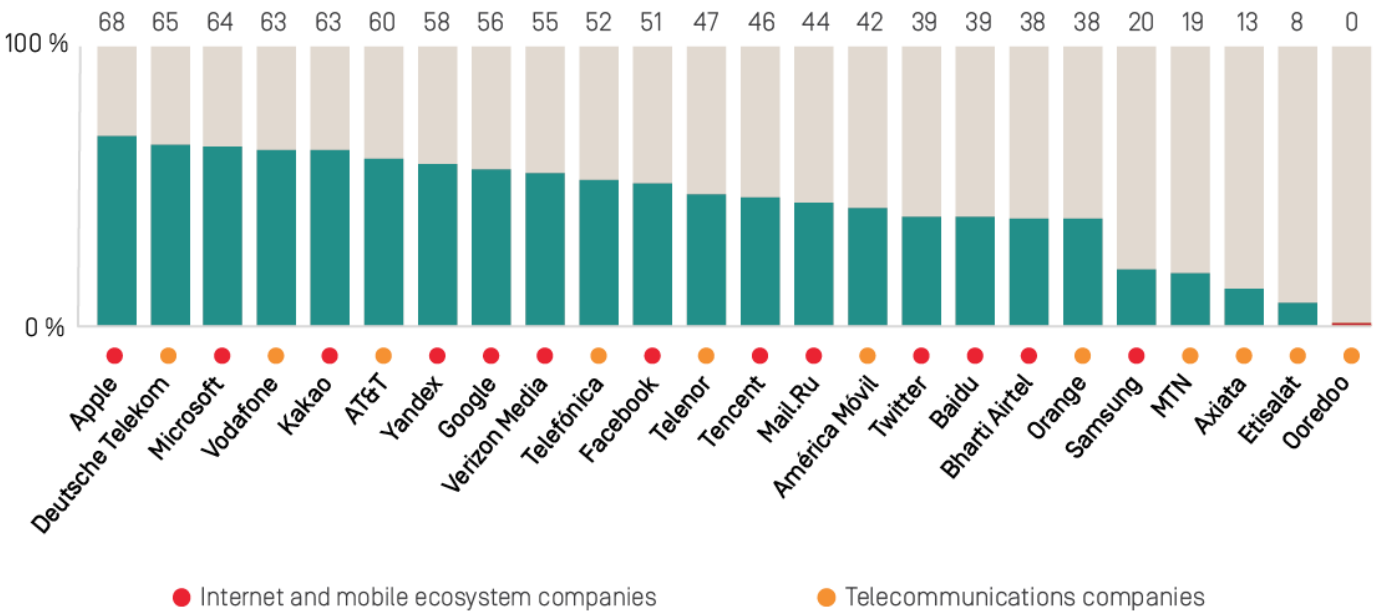
- **Security oversight:** The company should clearly disclose information about its institutional processes to ensure the security of its products and services, including limiting unauthorized employee access to user data (P13).

- **Security vulnerabilities:** The company should address security vulnerabilities when they are discovered (P14).
- **Data breaches:** The company should publicly disclose information about its processes for responding to data breaches (P15).
- **Security risks:** The company should publish information to help users defend themselves against cyber risks (P18).
- **Encryption** *(for internet and mobile ecosystem companies)*: The company should encrypt user communication and private content so users can control who has access to it (P16).
- **Account Security** *(for internet and mobile ecosystem companies)*: The company should help users keep their accounts secure (P17).

See the privacy indicators of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#P.**

As Figure 19 below shows, **Apple** received the best average score across the security indicators of any company in the RDR Index. It stood out for its strong encryption policies (P16)—which it improved over the last year. **Deutsche Telekom** received the highest score among telecommunications companies, and stood out for its strong disclosure of its security oversight systems (P13), and of its data breach policies (P15) relative to many of its peers.

Figure 19 | How transparent are companies about policies and practices for securing user information (P13-P18)?



Baidu and **Tencent** both made notable improvements in a number of areas—although both companies still scored poorly across these indicators overall. Both revealed more information about security oversight policies, including limits on employees' access to user data (P13), clarified their procedures for responding to data breaches (P15), and revealed that they use encryption for some of their services (P16).

Google was less transparent about its security policies than **Apple**, **Microsoft**, **Kakao**, and **Yandex**. While it earned the highest score for disclosing ways for users to keep their accounts secure (P17), it failed to disclose anything about its policies for handling data breaches (P15).

Facebook was less transparent than most of its U.S. peers—**Apple**, **Google**, **Microsoft**, and **Verizon Media**—about its security policies: it revealed little about its policies for limiting employee access to user data (P13), and disclosed nothing about its policies for handling data breaches (P15). But it earned above average marks for its encryption policies (P16): it clearly stated that for WhatsApp, end-to-end encryption is enabled by default, and that Messenger users can enable end-to-end encryption, although it is not enabled by default.

Twitter gave surprisingly little information about its security policies, scoring lower than all U.S. internet and mobile ecosystem companies on these indicators. Like most companies, it failed to disclose any information about how it responds to data breaches (P15). It also did not fully disclose what types of encryption are in place for Twitter (the social network) or Periscope (P16).

Notably, **Samsung** disclosed less than all internet and mobile ecosystem companies about its security policies. It disclosed nothing about its policies for responding to data breaches (P15), or about what types of encryption are in place to protect user information in transit or on Samsung devices (P16). It also lost points this year for failing to disclose if it made any modifications to the Android mobile operating system and how those changes might impact users' ability to receive security updates (P14).

Companies are becoming more transparent and accountable about how they handle data breaches—although most in the RDR Index still failed to disclose anything about their policies for addressing these incidents.

Data breaches continue to make headlines, growing both in number and in scope. More than 59,000 data breaches have been reported in Europe since the GDPR became applicable in May 2018.[80] In September 2018, hackers gained access to the data of up to 90 million Facebook users.[81] Also in 2018, India's biometric database, Aadhaar, suffered multiple breaches that exposed the personal records of more than 1 billion Indian citizens.[82]

Data breaches can occur as a result of malicious actors and external threats, as well as from so called "insider threats," which can be a result of poor internal security oversight.[83] However, even with strong security safeguards in place, companies can still experience breaches. And, these incidents not only pose a significant threat to individuals' financial and personal security—and risk the public's trust—they also hurt a company's bottom line: a data breach, on average, costs a company $3.86 million, according to a 2018 study by IBM.[84] That study also found that more serious breaches can cost hundreds of millions of dollars.

In response to the growing number of data breaches, the RDR Index in 2017 began evaluating how transparent companies are about their policies for handling these types of incidents. The 2017 RDR Index introduced a new indicator (P15) that evaluates company disclosure of their processes for responding to data breaches and of providing remedy to affected users.

How transparent are companies about their processes for handling data breaches?

What the RDR Index evaluates: Indicator P15 evaluates if a company clearly discloses a commitment to notify the relevant authorities without undue delay when a data breach occurs, if a company clearly discloses its process for notifying data subjects who might be affected by a data breach, and if a company explains what kinds of steps it will take to address the impact of a data breach on its users.

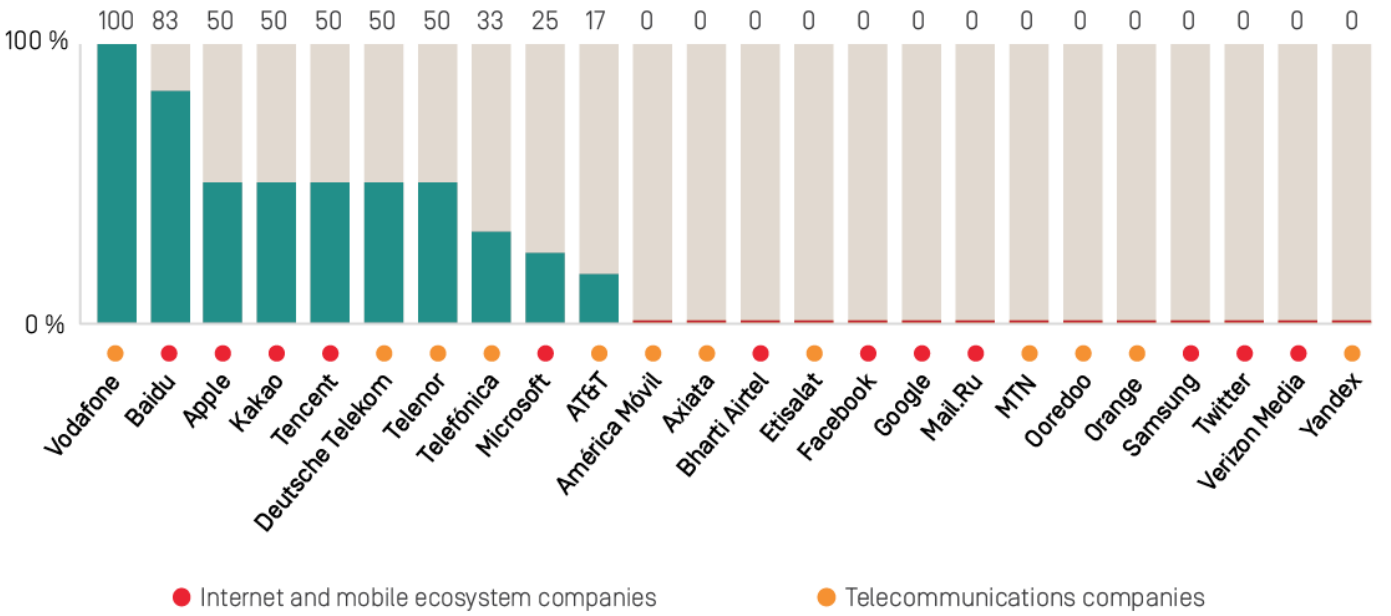
While many jurisdictions legally require companies to notify relevant authorities or take certain steps to mitigate the damage of data breaches, companies may not necessarily be legally compelled to disclose this information to the public or affected individuals. Even if there is a legal requirement to notify affected individuals, the exact definition of "affected individuals" can also vary significantly in different jurisdictions. However, regardless of whether the law is clear or comprehensive, companies that respect users' rights should clearly disclose when and how they will notify individuals who have been affected, or have likely been affected, by a data breach.

See the guidance for Indicator P15 of the RDR Index methodology: **rankingdigitalrights.org/2019-indicators/#P15**.

Results over the past three RDR Indexes indicate that companies are making steady progress. Data from the 2017 RDR Index showed that only three companies—**Telefónica**, **AT&T**, and **Vodafone**—disclosed anything about these processes. Telefónica revealed the most by committing to notify users in case of a breach and providing some information about steps for providing remedy. In the 2018 RDR Index, **Apple** joined this group—making it the only internet and mobile ecosystem company to receive any credit on Indicator P15—and Vodafone stood out for its comprehensive disclosure that earned it the top score on this indicator.

In this year's Index, 10 of the 24 companies evaluated earned some points on Indicator P15—a trend that appears to be driven by new regulations in various jurisdictions requiring companies to be more accountable for how they handle data breaches. As Figure 20 below shows, **Vodafone** was again the only company to receive a full score on this indicator. It disclosed a clear commitment to notify the relevant authorities without undue delay when a data breach occurs, provided details about its process for notifying data subjects who might be affected by a data breach, and explained what kinds of steps it will take to address the impact of a data breach on its users.[85]

Figure 20 | How transparent are companies about their processes for handling data breaches (P15)?



Both Chinese internet companies, **Baidu** and **Tencent**, received some credit on this indicator this year, likely due to stricter regulations in China requiring companies to have cybersecurity response plans that include user notification procedures.[86] Baidu received the highest score on this indicator among internet and mobile ecosystem companies, disclosing more than **Apple**, **Kakao**, **Tencent**, and **Microsoft**. Tencent tied with Apple and Kakao for the second-best score on this indicator, and disclosed more than Microsoft.

But six of the 12 internet and mobile ecosystem companies evaluated—including **Facebook**, **Google**, **Verizon Media**, and **Twitter**—still failed to disclose even basic information about what procedures they have in place to respond to data breaches in the event that such incidents occur. The striking lack of disclosure by most U.S. internet and mobile ecosystem companies—which collectively are responsible for securing troves of data about users globally—may be explained by the fact that there is no legal requirement in the U.S. pushing companies to be more transparent. However, both **Apple** and **Microsoft** stood out for providing some information about how they deal with data breaches even though they are not legally required to do so.

The same holds true for **Vodafone**. Its comprehensive disclosure is a laudable example of a company going beyond what is legally required of companies in the EU. The EU General Data Protection Regulation (GDPR)—which applies to all European telecommunications companies evaluated—requires "data controllers" to report breaches to authorities without "undue delay" and to notify affected users if the

company deems that the breach could result in a high risk to the person's privacy or security.[87] But there is no particular requirement for companies to formally disclose these policies under the GDPR. This may explain why disclosure by these companies was so inconsistent: **Deutsche Telekom**, **Telenor**, and **Telefónica** all disclosed some information but each disclosed different things; **Orange** disclosed nothing at all.

Encryption is essential for enabling and protecting online expression and privacy—but many companies do not disclose if they are protecting users with the highest level of encryption available.

Encryption and anonymity are essential to exercising and protecting human rights, both on and offline.[88] Yet over the last several years lawmakers around the world have passed measures undermining encryption—even giving authorities direct backdoors into user communications—in ways that human rights advocates say threaten fundamental privacy and freedom of expression rights.

For example, in Australia, the 2018 Assistance and Access Law gives broad authorities to the Australian government to compel tech companies to grant law enforcement agencies access to encrypted messages without the user's knowledge.[89] In the UK, the 2016 Investigatory Powers Act requires that network operators have the ability to "remove" end-to-end encryption.[90] In China, the 2016 Cybersecurity Law allows the government to force companies to decode encrypted data.[91] In Pakistan, the 2016 Prevention of Electronic Crimes Act criminalizes the use of encryption tools online.[92] And in India, the proposed Intermediary Guidelines legislation includes a provision that would undermine the use of encryption by companies like WhatsApp.[93]

Types of encryption

There are different types of encryption, depending on the security objective and the type of product or service.

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

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

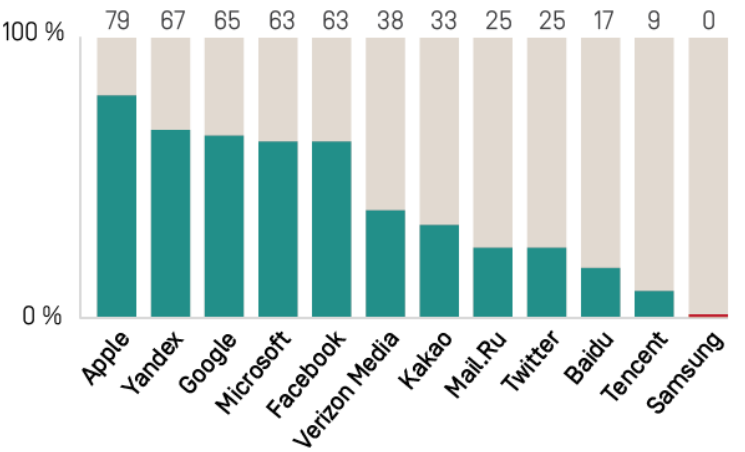
Forward secrecy is distinct from end-to-end encryption, which ensures that only the sender and intended recipient can read the content of the encrypted communications. Third parties, including the company, would not be able to decode the content. Many companies only encrypt traffic between users' devices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

See the RDR Index glossary of terms at: **rankingdigitalrights.org/2019-indicators**.

The RDR Index has one indicator (P16) that evaluates how transparent internet and mobile ecosystem companies are about their encryption policies.[94] Four elements measure if and how clearly companies disclose: if the transmission of user communications is encrypted by default; if the transmissions of user communications are encrypted using a unique key (what is referred to as "forward secrecy"); if users can secure their private content using end-to-end encryption (meaning not even the company can access the content); and if end-to-end encryption is enabled by default.

As Figure 21 below shows, **Apple** had the strongest encryption policies of any internet and mobile ecosystem company evaluated. It improved its disclosure of its encryption policies for iMessage and the iOS operating system, and clarified that it stores some user information in its iCloud cloud data service using end-to-end encryption so that even the company cannot access this data. As in previous years, the Russian internet company **Yandex** stood out for earning one of the top scores on this indicator, especially compared to the other Russian company in the RDR Index, **Mail.Ru**, which hardly disclosed any information about its encryption policies.

Figure 21 | How transparent are internet and mobile ecosystem companies about encryption standards (P16)?



Google earned the third-best score on this indicator, after **Apple** and **Yandex**: it disclosed that it encrypts user traffic by default, but did not provide an option for users to end-to-end encrypt their private content or communications for Gmail, YouTube, or Google Drive. In 2018, **Microsoft** rolled out end-to-end encryption for Outlook and Skype, giving users the option to end-to-end encrypt their private communications, although it is not enabled by default. It also provided OneDrive cloud service users with the option to end-to-end encrypt their private content. However, Microsoft failed to disclose whether the transmissions of data are encrypted with unique keys for Bing and Skype. **Facebook** provided end-to-end encryption by default for WhatsApp, and gave Messenger users the option to enable end-to-end encryption, although it is not on by default. In contrast, it failed to disclose any information about its encryption practices for Instagram.

As found in previous RDR Indexes, **Twitter** disclosed less about its encryption standards than all of its U.S. peers. The company revealed that for Twitter (the social network), users' internet traffic between their device and the company's servers is encrypted by default and with forward secrecy—but it did not disclose similar information for Periscope. It also did not indicate if direct messages on Twitter are end-to-end encrypted (or clearly disclose that these messages are not secure).

Baidu and **Tencent** communicated more about the encryption of user communication and private content than in previous years, although they still disclosed very little compared to their peers. Increased transparency by both companies in similar areas may be in response to new guidelines issued in May 2018 that elaborate standards for compliance with China's 2016 cybersecurity law.

Notably, **Samsung** remained the only company disclosing nothing about its encryption policies for either of the services evaluated (Android and Samsung Cloud). In contrast, its South Korean peer, **Kakao**, disclosed some information about its encryption policies for all three services evaluated (Daum Search, Daum Mail, and KakaoTalk). For KakaoTalk, it disclosed that users can encrypt their messages using end-to-end encryption, though this option is not on by default.

5.6 Regulatory trends and gaps

Companies should go beyond minimum legal requirements to ensure that users have control over what information is being collected and shared.

The EU's new data protection regulations that became applicable in May 2018 spurred similar regulations in some other countries around the world, and public pressure for stronger regulation in many more.[95] In China, lawmakers that same month issued guidelines reinforcing the country's data protection and cybersecurity laws, including new rules requiring companies to be more transparent about what data is collected, used, and shared.[96] In India, legislators in July 2018 submitted a draft bill that could

codify into law the country's landmark 2018 Supreme Court ruling that declared privacy a human right protected by India's constitution.[97] In South Africa, a new data protection law—modeled after the GDPR—is expected to take effect in 2019.[98]

In Europe, all 28 EU-member states are now bound by the GDPR's tougher regulations aimed at giving users greater control over their personal data. Meanwhile, the EU is set this year to finalize the e-Privacy Regulation (ePR)—the so-called "cookie" law—which will work in tandem with the GDPR to regulate online platforms, messaging and voice applications (such as Skype and WhatsApp), and e-commerce sites, and may require consent for the use of cookies and other tracking technologies.[99]

While varying in focus and scope, these measures have put a spotlight on the importance of data privacy—and reflect a consensus among lawmakers, the public, and even by companies themselves of the necessity for more responsible data protection practices and standards.

New data protection regulations enacted or proposed since 2018

The following is a (non-exhaustive) list of data protection regulations, proposed or enacted since 2018 in jurisdictions where the companies evaluated in the RDR Index are headquartered.

European Union: In May 2018 the General Data Protection Regulation (GDPR) became applicable. The regulation sets data protection standards for any company (or "data controller") that handles EU residents' personal information.

China: In May 2018, the Personal Information Security Specification came into effect.[101] Similar to GDPR principles, it clarifies the definition of personal information, and introduces obligations for how organizations should handle personal information. It sets guidelines for implementing China's existing data protection rules—notably the 2016 Cybersecurity Law.[102]

India: In July 2018, India introduced a draft Personal Data Protection Bill which, if passed, would recognize privacy as a fundamental right in line with a landmark 2018 ruling by India's Supreme Court.[103] The Bill establishes a comprehensive data protection framework for India that defines the data rights of individuals and an enforcement framework that includes a data protection authority. The Privacy, Security, and Ownership of the Data in the Telecom Sector recommendations—which recognize the impact of automated decision-making on privacy—were issued concurrently.[104]

South Africa: In December 2018 the long-anticipated Protection of Personal Information Act (POPI)[105] was officially published—although has yet to take effect. The law largely mirrors the GDPR, setting conditions for how companies should process personal information.

U.S. (California): The state of California passed a new law set to go into effect in January 2020 that grants Californians the right to be informed, at the time of personal information collection, what information is being collected and the purposes for which that information will be used.[106]

Results of the 2019 RDR Index are encouraging: most companies indeed appear to be taking concrete steps to do more to respect users' privacy. Most companies evaluated updated their policies to comply with regulatory demands, and these changes have resulted in improved clarity by most companies about how they handle and secure user data.

At the same time, some globally operating companies have responded to regional regulations in ways that resulted in uneven privacy protections for their users. As the GPDR became applicable in May 2018, Facebook, for instance, rolled out a different privacy policy for WhatsApp users in the EU, offering greater options to access and control their data—including rights to export and delete their information. Notably, the U.S. version of WhatsApp does not offer those users the same options and rights as EU-based WhatsApp users, since U.S. users are not legally covered under the GDPR.

Results also reveal key areas where companies are making no or little progress—particularly around privacy-related issues where there are weak or no regulations pushing companies to improve. This is especially evident among European telecommunications companies—which, although bound by stricter data protection regulations under the GDPR, still lacked transparency around key issues affecting users' privacy.

It is critical to note that the RDR Index does not evaluate a company's GDPR compliance. The RDR Index evaluates how transparent companies are about relevant policies affecting users' privacy based on 18 indicators in the RDR Index—a subset of which loosely overlap with certain GDPR provisions and principles related to obligations about handling user data. But the RDR Index evaluates a much wider range of privacy-related issues than are addressed by the GDPR—including how transparent companies are about how they handle government demands for user data and about their security policies and practices. And, while both the RDR Index and the GDPR draw from and encourage compliance with the same set of international human rights principles and frameworks that guarantee privacy as a universal human right, the RDR Index requires companies to publicly disclose their commitments and policies in this regard, whereas the GDPR does not consistently incorporate the same high standards of disclosure.

Meanwhile, the GDPR establishes minimum standards for how "data controllers"—in this case, companies—should disclose regarding their handling of personal data.[107] But

national regulations and individual companies can, and in many cases *should*, go beyond the GDPR's minimum transparency requirements. Only then can users be better informed of what is happening to their data—as well as understand the risks associated with using a particular service or product—in order to make informed choices. Our results in fact show that European telecommunications companies that performed best on the RDR Index on different indicators in the Privacy category were those that went beyond the GDPR's minimum requirements and disclosed more detail about how they handle and secure user information.

An example is the GDPR's notification requirements regarding data breaches. The GDPR requires "data controllers" to report breaches to authorities without "undue delay" and to notify affected users if the company deems that the breach could result in a high risk to the person's privacy or security.[108] But companies are not necessarily required to publish a policy that describes their protocols for handling these incidents, or to publicly commit to notify or provide remedy to affected users—as is the standard set by the RDR Index. Indicator P15 of the RDR Index expects companies to clearly disclose their policies for responding to data breaches, including clearly committing to notifying affected users and detailing what steps they will take to address the impacts. In the absence of this disclosure, a victim of a data breach would have no idea what steps the company takes after a breach has occurred or how to hold a company accountable in case these steps are not followed. **Vodafone** stood out as an example of a company that went beyond the GDPR's minimum requirements pertaining to data breaches by publishing a policy clearly outlining its process for handling data breaches, including its procedures for notifying authorities, and affected users, as well as describing its policies for providing remedy when these incidents occur.

Another key gap in the GDPR is around government demands. The scope of the GDPR specifically excludes this aspect of data privacy, which means companies are not obliged under the GDPR to disclose their relationships with governments or law enforcement, or their processes for responding to government demands to hand over or otherwise access user information.[109] The RDR Index, however, expects robust transparency in these areas. While we recognize that telecommunications companies in Europe and in many jurisdictions around the world are often prohibited by national security laws from disclosing actual data about the government demands they receive and comply with, we expect companies to publish as much information as is legally permissible. At the very least, companies should explain their *processes* for handling such requests—which typically is not legally prohibited, even in the most restrictive environments—and, ideally, publish data revealing the number and types of requests they receive and comply with and to commit to informing users when their data has been requested. Companies should clearly specify the legal reasons preventing them from being fully transparent in these areas. Notably, these transparency standards follow industry best practices, including those set by GNI.[110]

Meanwhile, the proposed e-Privacy Regulation (ePR) may address at least some of these gaps—or so many experts and advocates hope.[111] The regulation is intended to fill in

details about how "data controllers" should implement and comply with the GDPR, and will also cover a range of issues that fall outside the GDPR's current scope. Some advocacy groups, including Access Now, are pushing to include requirements for companies to publish yearly transparency reports about how they handle government demands, and to provide users clear avenues to seek remedy in case of privacy abuses.[112]

5.7 Recommendations for companies

1. Go beyond legal compliance: Regulations alone do not ensure that companies are doing enough to respect users' privacy. Companies should go beyond what may be legally required to ensure they are protecting and respecting users' fundamental human right to privacy.

2. Maximize transparency: Companies should disclose the maximum possible information about policies affecting users' privacy, including their handling of user information and options users have to control what data is collected, shared, and how it is used. Companies should supply users with the information they need to give meaningful consent for how their data is managed.

3. Disclose government demands: Companies should publish regular transparency reports, including descriptions and data about actions they take in response to government demands to hand over user information, and disclose any legal reasons preventing them from being fully transparent in this area. They should also commit to notifying users when their data has been requested or provide legal justifications for when they are unable to do so.

4. Demonstrate a credible commitment to security: Companies should disclose whether and to what extent they follow industry standards of encryption and security, conduct security audits, monitor employee access to information, and educate users about threats.

5. Strengthen governance of privacy commitments: Implement effective governance and oversight of risks to users' privacy posed by governments as well as by all other types of actors who may gain access to their information. Provide accessible, predictable, and transparent grievance and remedy mechanisms that ensure effective redress for violations of privacy, in line with the U.N. Guiding Principles on Business and Human Rights.

6. Apply privacy protections universally: Companies should implement privacy policies that offer the highest possible protections in all of the markets in which they operate, respecting the human rights of all users equally, regardless of geographic location.

5.8 Recommendations for governments

1. Prioritize transparency: Privacy laws and data protection regulations should include strong transparency and disclosure requirements so that users can make informed decisions about whether and how to use a product or service, and exercise meaningful control over how a company can use their information.

2. Reform surveillance laws: Surveillance-related laws and practices should be reformed to comply with the 13 "Necessary and Proportionate" principles,[113] a framework for assessing whether current or proposed surveillance laws and practices are compatible with international human rights norms.

3. Be transparent: Governments should publish accessible information and relevant data about all requirements and demands made by government entities (national, regional, and local) to hand over or otherwise access user data. For government members of the Open Government Partnership—an organization dedicated to making governments more open, accountable, and responsive to citizens—transparency about requests and demands made to companies affecting privacy should be considered a fundamental part of that commitment.

4. Support encryption: Governments should not weaken or undermine encryption standards, ban or limit users' access to encryption, or enact legislation requiring companies to provide "backdoors" or vulnerabilities that allow for third-party access to unencrypted data, or to hand over encryption keys.

5. Require strong corporate governance: As described in Chapter 3, governments should require companies to carry out credible due diligence, assessing the impact and risks of their operations and policies on users' privacy. Companies should also be required to provide meaningful grievance and remedy mechanisms, and to ensure that the law enables meaningful legal recourse and remedy for violations of privacy.

6. Engage with stakeholders: Work with civil society, companies, and other governments to develop and enforce effective, constructive regulation that prioritizes the human rights of all internet users.

6. Questions for investors

The RDR Index methodology provides a clear standard for investors to use in evaluating company respect for users' digital rights.[114] How comprehensive are companies' efforts to mitigate risks to their business? How clearly do they show that they are working to anticipate and reduce potential privacy or freedom of expression risks faced by those who use their technologies, platforms, and services?

Shareholder value is put at risk not only by security breaches, but also when companies fail to identify and mitigate broader risks to user privacy across their business operations. Companies also face risks when they fail to anticipate and address content-related issues spanning from incitement to violence and targeted disinformation campaigns, to government censorship and network shutdowns.

Over the past two years, many government regulatory initiatives have emerged quickly in response to breaches, scandals, and tragedies. The current momentum in the United States for national privacy regulation was not expected by analysts and pundits even a year ago. In response to recent terror attacks and continued concerns about cross-border disinformation campaigns during sensitive election periods, efforts to regulate information flows through telecommunications networks and content appearing on internet platforms are also proliferating in a range of countries. It is clear that if companies merely focus on compliance with existing and widely anticipated regulations, they are not doing enough to protect themselves from long-term regulatory risk.

The RDR Index indicators represent a concrete standard not only for companies to meet their normative responsibility to respect human rights, but also for moving beyond compliance and getting ahead of regulatory risks. Companies in the sector that build their policies and practices around transparency, accountability, and respect for users' human rights will be in a better position to identify and mitigate harms to individuals and communities that regulators will eventually be compelled to address. Usually, by the time regulatory intervention becomes necessary to address a problem, that problem will have already become entrenched and widespread, making compliance much more costly.

The following 12 categories of questions are offered as guidance for investor due diligence about whether companies are making adequate efforts to respect users' rights, thereby mitigating individual harms and broader business risks. These questions are also a useful starting point for investor engagement with companies, particularly when combined with key findings and recommendations from the individual company report cards.

1. Oversight: Does the board of directors exercise direct oversight over risks related to users' security, privacy, and freedom of expression? Does board membership include people with expertise and experience on issues related to digital rights? (Indicator G2)

2. Risk assessment: Has the company management identified digital rights risks that are material to its business—or which may become material in the future? Does the company carry out human rights impact assessments on the full range of ways that its products and services may affect users' human rights, including risks associated with the deployment of algorithms and machine learning? Does it disclose any information about whether and how the results of assessments are used? Are the assessments assured by an independent third party? (Indicator G4)

3. Business model: Does the company evaluate and disclose risks to users' human rights that may result from its business model, particularly targeted advertising? Does it evaluate tradeoffs being made between profit and risk, such as sharing of user data with commercial partners versus strong data controls? (Indicator G4)

4. Stakeholder engagement and accountability: Is the company a member of the Global Network Initiative (GNI) and if not, why not? Does it engage with vulnerable communities in the course of developing and conducting its risk assessment processes, developing and enforcing terms of service, and developing as well as implementing grievance and remedy mechanisms? (Indicator G5)

5. Grievance and remedy: Does the company disclose accessible and meaningful mechanisms for users to file grievances and obtain remedy when their freedom of expression or privacy rights are infringed in relation to the company's product or service? (Indicator G6)

6. Transparency about data collection and use: Regardless of whether a company claims to be compliant with relevant law, does it disclose clear information about its policies and practices regarding collection, use, sharing, and retention of information that could be used to identify, profile, or track its users? (Indicators P1-P12)

7. Transparency about handling of government demands and other third-party requests affecting users' freedom of expression and privacy rights: Does the company disclose policies for how it handles all types of third-party requests to provide access to user data, restrict content, restrict access, or shut down service? (Indicators F5-F7, and P10-P12)

8. Publication of transparency data: Does the company publish regular data about the volume and nature of the requests it receives, and responds to, for sharing user data, restricting content or accounts, or shutting down networks? Does it also publish data about the volume and nature of content and accounts restricted in the course of enforcing its own terms of service? (Indicators F6, F7, and P11)

9. Evidence of strong policies for addressing security vulnerabilities: Does the company disclose clear information about policies for addressing security vulnerabilities, including the company's practices for relaying security updates to mobile phones? (Indicator P14)

10. Encryption: Does the company commit to implement the highest encryption standards available for the particular product or service? If not, why not? (Indicator P16)

11. Mobile security: Do companies that operate mobile ecosystems disclose clear policies about privacy and security requirements for third-party apps? (Indicators P1-P8)

12. Telecommunications transparency about network management: Do telecommunications companies disclose whether they prioritize, block, or delay applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network? If yes, do they disclose the purpose for doing so? (Indicator F9)

To view each company's "report card": **rankingdigitalrights.org/index2019/companies**.

7. Appendix

7.1 RDR Index methodology development

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

For more information about the RDR Index methodology development, see: rankingdigitalrights.org/methodology-development.

To view or download the full 2019 RDR Index methodology, visit: rankingdigitalrights.org/2019-indicators.

Looking ahead: Following the launch of the 2019 RDR Index, we plan to expand our methodology to address human rights harms associated with targeted advertising, algorithms, and machine learning. We will also adapt the methodology to include more company types, like powerful global platforms with core e-commerce businesses such as Amazon and Alibaba. The fifth RDR Index, with the expanded methodology and scope, will be published in 2021.

To learn more about the 2021 RDR Index methodology development process, see: **rankingdigitalrights.org/methodology-development/2021-revisions.**

7.2 Company selection

The 2019 RDR Index evaluates 12 telecommunications companies and 12 internet and mobile ecosystem companies. All companies evaluated are multinational corporations listed on a major stock exchange. The following factors influenced company selection:

- **User base:** The companies in the RDR 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 and mobile ecosystem companies have a

large number of global users as identified by established global traffic rankings such as Alexa. The policies and practices of the selected companies, and their potential to improve, thus affect a large percentage of the world's 4.3 billion internet users.[115]

- **Geographic reach and distribution:** The RDR Index includes companies that are headquartered in North America, Europe, Africa, Asia, and the Middle East.
- **Relevance to users' freedom of expression and privacy rights:** Most of the companies in the RDR 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.

7.3 Selection of services

The following factors guided the selection of services:

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

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

Mobile ecosystems: Most of the world's mobile devices are running either on Apple's iOS operating system, or some version of Google's Android mobile operating system. Thus we evaluate Apple's iOS ecosystem plus two different variants of the Android ecosystem: Android on devices controlled directly by Google (the Nexus smartphone and Pixel tablet product lines), and Android on devices controlled by Samsung.

7.4 Levels of disclosure

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

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

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

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

7.5 Research process and steps

RDR works with a network of international researchers to collect data on each company, and to evaluate company policies in the language of the company's operating market. RDR's external research team for the 2019 RDR Index consisted of 32 researchers from 17 countries. A list of our partners and contributors can be found at: rankingdigitalrights.org/who/affiliates.

The research process for the 2019 RDR Index consisted of several steps involving rigorous cross-checking and internal and external review, as follows:

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

7.6 Company engagement

Proactive and open stakeholder engagement has been a critical component of RDR's work and of the RDR Index methodology. As such, we communicated with companies throughout the research process.

Open dialogue and communication. Before the research began, we contacted all 24 companies and informed them that they were included in this year's RDR Index, describing our research process and timeline. Following several stages of research and review, we shared each company's initial results with them. We invited companies to provide written feedback as well as additional source documents. In many cases, the research team conducted conference calls or meetings with companies that requested them to discuss the initial findings as well as broader questions about the RDR Index and its methodology

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

7.7 Scoring

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

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

Points

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

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

Governance category scoring

- G1, G5:
  - Internet and mobile ecosystem companies' scores were based on the group-level scores.
  - Telecommunications companies' scores were based on average group-level and operating company scores.
- G2, G3, G4:
  - Internet and mobile ecosystem companies' scores were based on average of group-level and services scores.
  - Telecommunications companies' scores were based on average of group-level, operating, and services scores.
- G6:
  - Internet and mobile ecosystem companies's scores were based on average of service-level scores.
  - Telecommunications companies's scores were based on average of service-level scores.

Indicator and element scoring

Telecommunications companies were evaluated on 32 of the 35 indicators; internet and mobile ecosystem companies were evaluated on 33 of the 35 indicators. Some elements within indicators were not applicable to certain services. The following list identifies which indicators or elements were N/A for certain companies or services:

F3, Element 2: N/A for search engines

- F3, Elements 4-5: N/A for prepaid and postpaid mobile services, cloud service, email services, and messaging services
- F5-F7: N/A for email services
- F6, Element 2: N/A for search engines
- F7, Element 2:N/A for search engines
- F6, Element 3: N/A for messaging services
- F7, Element 3: N/A for messaging services
- F8, Element 1: N/A for telecommunications companies
- F8, Elements 1 & 4: N/A for search engines
- F8, Elements 1-3: N/A for email services
- F9: N/A for internet and mobile ecosystem companies
- F10: N/A for internet and mobile ecosystem companies
- F11: N/A for postpaid mobile and fixed-line internet services and search engines
- P9: N/A for telecommunications companies
- P14, Elements 5, 6, 9: N/A for internet companies and Google and Apple mobile ecosystems, and fixed-line broadband services
- P14, Elements 4, 7, 8: N/A for internet companies and telecommunications companies
- P16: N/A for telecommunications companies
- P16, Elements 3-4: N/A for internet services without private messaging functions
- P17: N/A for telecommunications companies and search engines

The following elements apply only to mobile ecosystems:

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

7.8 For further information

The 2015 RDR Index can be viewed here: rankingdigitalrights.org/index2015

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

The 2018 RDR Index can be viewed here: rankingdigitalrights.org/index2018

Acknowledgments

Ranking Digital Rights staff:

- Rebecca MacKinnon, Director
- Amy Brouillette, Research Director
- Lisa Gutermuth, Senior Program Manager
- Laura Reed, Research and Engagement Manager
- Nathalie Maréchal, Senior Research Analyst
- Veszna Wessenauer, Research Analyst
- Afef Abrougui, Corporate Accountability Editor
- Sam Cabral, Communications Associate
- Ilja Sperling, Student Worker
- Zak Rogoff, Research Fellow
- Eeva Moore, Editor and Publications Coordinator

We wish to thank all stakeholders who provided key feedback on the 2019 RDR Index methodology. We also wish to thank those who offered key feedback about this report and the findings: Joan Barata, Melissa Brown, Sharon Bradford Franklin, Bennett Freeman, Djordje Krivokapic, Emma Llansó, Deirdre K. Mulligan, Courtney Radsch.

Contributing researchers: Shazeda Ahmed, Ope Akanbi, Mariam Al Shafie, Mariia Altergot, Grant Baker, Joan Barata, Alex Comninos, David Martín Espitia, Luis Fernando García, Krzysztof Garstka, Kirsten Gollatz, Elonnai Hickok, Jockum Hildén, Maria Fonneløp Inderberg, Abed Kataya, Kelly Kim, Priya Kumar, Cannelle Lavite, Tanya Lokot, Kirill Miazine, Outi Puukko, Kjetil Wick Sætre, Mingli Shi, Jiwon Son, Florian Wittner, Hu Yong, Benjamin Zhou.

Graphics: Olivia Solis, SHARE Lab

About Ranking Digital Rights

Ranking Digital Rights is a non-profit research initiative housed at the New America Foundation's Open Technology Institute. We work to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights. We do this by ranking the world's most powerful

internet, mobile ecosystem, and telecommunications companies on relevant commitments and policies, based on international human rights standards. We work with companies as well as advocates, researchers, investors, and policymakers to establish and advance global standards for corporate accountability. For more about our vision, impact, and strategy see: rankingdigitalrights.org/about/

For more about Ranking Digital Rights and the RDR Corporate Accountability Index, please visit www.rankingdigitalrights.org.

For more about New America, please visit www.newamerica.org.

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

Funders

The 2019 Corporate Accountability Index was supported by the following funders: John D. and Catherine T. MacArthur Foundation • Ford Foundation • Mozilla Foundation • Open Society Foundations • U.S. Department of State, Bureau of Democracy, Human Rights, and Labor. For a full list of current and former project funders and partners, please see: rankingdigitalrights.org/who/partners.

Notes

[1] Figures as of April 18, 2019. Bloomberg Markets, www.bloomberg.com/markets.

[2] Figures as of March 31, 2019. "World Internet Users Statistics and 2019 Population Stats," Internet World Stats, accessed April 23,2019, www.internetworldstats.com/stats.htm.

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

[4] See the 2019 RDR Index methodology at: rankingdigitalrights.org/2019-indicators

[5] "Guiding Principles on Business and Human Rights" (United Nations, 2011), www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[6] "Principles," Global Network Initiative, accessed February 27, 2017, globalnetworkinitiative.org/gni-principles

[7] "Implementation Guidelines," Global Network Initiative, accessed February 28, 2017, globalnetworkinitiative.org/implementation-guidelines

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

[9] For the full set of indicators, definitions, and research guidance please visit: "2019 Indicators," Ranking Digital Rights, rankingdigitalrights.org/2019-indicators

[10] "2019 Indicators: Governance," Ranking Digital Rights, rankingdigitalrights.org/2019-indicators/#G

[11] "2019 Indicators: Freedom of Expression," Ranking Digital Rights, rankingdigitalrights.org/2019-indicators/#F

[12] "2019 Indicators: Privacy," Ranking Digital Rights, rankingdigitalrights.org/2019-indicators/#P

[13] Catharine Smith, "Egypt's Facebook Revolution: Wael Ghonim Thanks The Social Network," *Huffington Post*, February 11, 2011, www.huffpost.com/entry/egypt-facebook-revolution-wael-ghonim_n_822078

[14] See Freedom on the Net 2018, Freedom House, freedomhouse.org/report/freedom-net/freedom-net-2018, 2019 World Press Freedom Index, Reporters Without Borders, rsf.org/en/ranking, and the EIU Democracy Index, The Economist Intelligence Unit, www.eiu.com/topic/democracy-index.

[15] Carole Cadwalladr, "My TED talk: how I took on the tech titans in their lair," *The Guardian*, April 21, 2019, www.theguardian.com/uk-news/2019/apr/21/carole-cadwalladr-ted-tech-google-facebook-zuckerberg-silicon-valley.

[16] State of Civil Society Report 2019, CIVICUS, www.civicus.org/index.php/state-of-civil-society-report-2019.

[17] "Guiding Principles on Business and Human Rights" (United Nations, 2011), www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf.

[18] The Case for the Web report, World Wide Web Foundation, webfoundation.org/research/the-case-for-the-web/.

[19] "2019 Internet Society Global Internet Report: Consolidation in the Global Economy" (Internet Society, 2019),future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf.

[20] Internet Health Report 2019, Mozilla Foundation, internethealthreport.org/2019/.

[21] Paul Sandle, "Web creator Berners-Lee launches contract for better internet," *Reuters*, November 6, 2018, www.reuters.com/article/us-portugal-websummit-berners-lee/web-creator-berners-lee-launches-contract-for-better-internet-idUSKCN1NA2CX.

[22] Bennett Freeman et al, "New guidance for companies encourages action to support civic freedoms & human rights defenders & explores opportunities for engagement," Business & Human Rights Resource Centre, August 29, 2018, www.business-humanrights.org/en/new-guidance-for-companies-encourages-action-to-support-civic-freedoms-human-rights-defenders-explores-opportunities-for-engagement.

[23] "The GNI Principles," Global Network Initiative, accessed April 22, 2019, globalnetworkinitiative.org/gni-principles/.

[24] "Facebook says it was 'too slow' to fight hate speech in Myanmar," Reuters, August 16, 2018, www.cnbc.com/2018/08/16/facebook-says-it-was-too-slow-to-fight-hate-speech-in-myanmar.html; Ariana Tobin, Madeleine Varner, and Julia Angwin, "Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up," ProPublica, December 28, 2017, www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes; Michelle Castillo, "Facebook's Mark Zuckerberg: 'I'm responsible for what happened' with data privacy issues," CNBC, April 4, 2018, www.cnbc.com/2018/04/04/mark-zuckerberg-facebook-user-privacy-issues-my-mistake.html.

[25] "Community Standards Enforcement Report," Facebook, accessed April 22, 2019, transparency.facebook.com/community-standards-enforcement.

[26] "National Standards on Information Security Technology – Personal Information Security Specification GB/T 35273-2017 ("PI Specification")," (Standardization Administration of China, May 2018), www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE

[27] "Year-on-year Comparison," 2018 Ranking Digital Rights Corporate Accountability Index, rankingdigitalrights.org/index2018/compare

[28] "Governance advances and gaps," 2018 Ranking Digital Rights Corporate Accountability Index, rankingdigitalrights.org/index2018/report/inadequate-disclosure/#section-33

[29] Altschuller, Sarah A and Amy K Lehr, "The French Duty of Vigilance Law: What You Need to Know," Corporate Social Responsibility and the Law, August 3, 2017, www.csrandthelaw.com/2017/08/03/the-french-duty-of-vigilance-law-what-you-need-to-know

[30] "Privacy," Apple, accessed April 22, 2019, www.apple.com/lae/privacy

[31] "About Yandex," Yandex, accessed April 22, 2019, yandex.com/company/general_info/yandex_today

[32] "Human Rights Policy," (América Móvil, 2018), s22.q4cdn.com/604986553/files/doc_downloads/human_rights/Human-Rights-Policy.pdf and "2017 Sustainability Report," (América Móvil, 2018), s22.q4cdn.com/604986553/files/doc_downloads/sustainability/sustainability-report-2017.pdf

[33]"A/HRC/29/32: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (United Nations Human Rights Council, May 22, 2015), ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32.

[34] See the 2019 RDR Index glossary at: rankingdigitalrights.org/2019-indicators/#hria

[35] See the 2019 RDR Index methodology at: rankingdigitalrights.org/index2019/indicators/G4

[36] Verena Fulde, "Deutsche Telekom's guidelines for artificial intelligence," Deutsche Telekom, accessed April 22, 2019, www.telekom.com/en/company/digital-responsibility/details/artificial-intelligence-ai-guideline-524366.

[37] "G6: Remedy," 2018 Ranking Digital Rights Corporate Accountability Index, rankingdigitalrights.org/index2018/indicators/G6

[38] "National Action Plan," Business & Human Rights Resource Center, accessed April 22, 2019, www.business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-governments/by-type-of-initiative/national-action-plans

[39] Peter Micek, "New U.S. plan for responsible business conduct takes baby steps toward digital rights," Access Now, January 30, 2017, www.accessnow.org/new-u-s-plan-responsible-business-conduct-takes-steps-toward-digital-rights

[40] "Non-financial reporting," European Commission, accessed April 22, 2019, ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en

[41] "Companies failing to report meaningful information about their impacts on society and the environment," Alliance for Corporate Transparency, February 8, 2019, www.allianceforcorporatetransparency.org/news/companies-failing.html

[42] Altschuller, Sarah A and Amy K Lehr, "The French Duty of Vigilance Law: What You Need to Know," Corporate Social Responsibility and the Law, August 3, 2017, www.csrandthelaw.com/2017/08/03/the-french-duty-of-vigilance-law-what-you-need-to-know

[43] “German Development Ministry drafts law on mandatory human rights due diligence for German companies,” Business & Human Rights Resource Centre, accessed April 22, 2019, www.business-humanrights.org/en/german-development-ministry-drafts-law-on-mandatory-human-rights-due-diligence-for-german-companies

[44] Benjamin Fox, “Table human rights due diligence law, MEPs tell Commission,” Euractiv, March 28, 2019, www.euractiv.com/section/energy-environment/news/table-human-rights-due-diligence-law-meps-tell-commission

[45] “Investors representing $1.3 trillion voice support for legislation to mainstream ESG risk management in global financial systems,” Investor Alliance for Human Rights, March 25, 2019, investorsforhumanrights.org/news/investors-representing-13-trillion-voice-support-legislation-mainstream-esg-risk-management

[46] Ghosh, Dipayan and Ben Scott, “Digital Deceit: The Technologies Behind Precision Propaganda on the Internet,” New America Public Interest Technology, January 23, 2018, www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/ and Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019), www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781478947271/.

[47] Vishal Manve, “Twitter Tells Kashmiri Journalists and Activists That They Will Be Censored at Indian Government's Request,” Global Voices, September 14, 2017, advox.globalvoices.org/2017/09/14/kashmiri-journalists-and-activists-face-twitter-censorship-at-indian-governments-request/ and “Germany: Flawed Social Media Law,” Human Rights Watch, February 14, 2018, www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

[48] Rebecca MacKinnon et al, “Fostering Freedom Online: The Role of Internet Intermediaries” (UNESCO, 2014), www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/fostering-freedom-online-the-role-of-internet-intermediaries/

[49] “Removal requests,” Twitter Transparency Report, transparency.twitter.com/en/removal-requests.html.

[50] “Government requests to remove content,” Google Transparency Report, transparencyreport.google.com/government-removals/overview?hl=en.

[51] Jim Killock, “UK Internet Regulation – Part I: Internet Censorship in the UK today” (Open Rights Group, December 18, 2018), www.openrightsgroup.org/about/reports/uk-internet-regulation.

[52] “Keep It On,” Access Now, accessed April 22, 2019, www.accessnow.org/keepiton/.

[53] “The Freedom Online Coalition Joint Statement on State Sponsored Network Disruptions” (Freedom Online Coalition, 2017), www.freedomonlinecoalition.com/wp-content/uploads/2017/03/FOCJointStatementonStateSponsoredNetworkDisruptions.docx.pdf.

[54] Damien Cave, “Australia Passes Law to Punish Social Media Companies for Violent Posts,” The New York Times, April 3, 2019, www.nytimes.com/2019/04/03/world/australia/social-media-law.html.

[55] Leonid Bershidsky, “Disrespect Putin and You'll Pay a $23,000 Fine, “ Bloomberg, March 14, 2019, www.bloomberg.com/opinion/articles/2019-03-14/russian-censorship-laws and James Griffiths, “China's censors face a major test in 2019. But they've spent three decades getting ready,” CNN, January 7, 2019, www.cnn.com/2019/01/04/asia/china-internet-censorship-2019-intl/index.html.

[56] “Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online” (European Commission, September 12, 2018), ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf.

[57] “Directive (EU) 2019/... of the European Parliament and of the Council on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC” (European Parliament, March 26, 2019, www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0231+0+DOC+XML+V0//EN#BKMD-16.

[58] “Proposition de Loi Relative À La Lutte Contre La Manipulation de L’information” (Assemblée Nationale, November 20, 2018), www.assemblee-nationale.fr/15/ta/tap0190.pdf; Also see Alexander Damiano Ricci, “French opposition parties are taking Macron’s anti-misinformation law to court,” Poynter, December 4, 2018, www.poynter.org/fact-checking/2018/french-opposition-parties-are-taking-macrons-anti-misinformation-law-to-court/.

[59] “Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)” (Bundestag, June 12, 2018), bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.

[60] “Online Harms White Paper” (Department for Digital, Culture, Media & Sport et al, April 8, 2019), www.gov.uk/government/consultations/online-harms-white-paper.

[61] “Regulation on Security Assessment of Internet Information Services Having Public-Opinion Attributes or Social Mobilization Capabilities” (Cyberspace Administration of China, November 15, 2018), www.cac.gov.cn/2018-11/15/c_1123716072.htm.

[62] “The Information Technology [Intermediaries Guidelines (Amendment) Rules]” (Ministry of Electronics and Information Technology, December 24, 2018), meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

[63]“Bill No. 608767-7: On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"” (State Duma Committee on Information Policy, Information Technologies and Communications, April 22, 2019, sozd.duma.gov.ru/bill/608767-7?fbclid=IwAR2LHSnuRHxrEmP7ooOyVVJzhuKySbNNUXmLgJuOFbesKbN.

[64] Rebecca MacKinnon et al, “Fostering Freedom Online: The Role of Internet Intermediaries” (UNESCO, 2014),

www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/fostering-freedom-online-the-role-of-internet-intermediaries/ and "A Human Rights Approach to Platform Content Regulation," Freedex, April 2018, freedex.org/a-human-rights-approach-to-platform-content-regulation/.

[65] Rebecca MacKinnon et al, "Fostering Freedom Online: The Role of Internet Intermediaries" (UNESCO, 2014).

[66] See for example: Thant Sin, "Facebook Bans Racist Word 'Kalar' In Myanmar, Triggers Collateral Censorship," Global Voices Advox, June 2, 2017, advox.globalvoices.org/2017/06/02/facebook-bans-racist-word-kalar-in-myanmar-triggers-collateral-censorship/ and The DiDi Delgado, "Mark Zuckerberg Hates Black People," Medium, May 18, 2017, medium.com/@thedididelgado/mark-zuckerberg-hates-black-people-ae65426e3d2a.

[67] Hogan, Libby and Michael Safi, "Revealed: Facebook hate speech exploded in Myanmar during Rohingya crisis," The Guardian, April 3, 2018, www.theguardian.com/world/2018/apr/03/revealed-facebook-hate-speech-exploded-in-myanmar-during-rohingya-crisis.

[68]Tarleton Gillespie, "How Social Networks Set the Limits of What We Can Say Online," WIRED, June 26, 2018, www.wired.com/story/how-social-networks-set-the-limits-of-what-we-can-say-online/.

[69]"A Human Rights Approach to Platform Content Regulation," Freedex, April 2018, freedex.org/a-human-rights-approach-to-platform-content-regulation/.

[70] "2019 Indicators: Privacy," Ranking Digital Rights, rankingdigitalrights.org/2019-indicators/#P.

[71] "2018 Ranking Digital Rights Corporate Accountability Index" (Ranking Digital Rights, 2018), rankingdigitalrights.org/index2018/assets/static/download/RDRindex2018report.pdf.

[72] "Information Security Technology – Personal Information Security Specification (GB/T 35273-2017)" (Standardization Administration of China, May 2018).

[73] See the 2019 RDR Index methodology at: rankingdigitalrights.org/2019-indicators/.

[74] See the 2019 RDR Index methodology at: rankingdigitalrights.org/2019-indicators/#P7.

[75] "Targeted Advertising and Lack of User Control," 2018 Ranking Digital Rights Corporate Accountability Index, rankingdigitalrights.org/index2018/report/privacy-failures/#section-53.

[76] Freedom on the Net 2018, Freedom House, freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

[77] "H.R. 2048 - USA Freedom Act of 2015" (114th Congress, 2015), www.congress.gov/bill/114th-congress/house-bill/2048.

[78] "How do we share, transfer, and publicly disclose your personal information?" Baidu Privacy Policy, accessed April 25, 2019, www.baidu.com/duty/yinsiquan-policy.html.

[79] Kurt Wagner, "Facebook employees had access to private passwords for hundreds of millions of people," Recode, March 21, 2019, www.recode.net/2019/3/21/18275917/facebook-passwords-privacy-encryption-employees-access.

[80] "DLA Piper GDPR data breach survey: February 2019," DLA Piper, February 6, 2019, www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/.

[81] Aja Romano, "Facebook says 50 million user accounts were exposed to hackers," Vox, September 28, 2019, www.vox.com/2018/9/28/17914598/facebook-new-hack-data-breach-50-million.

[82] Vidhi Doshi, "A security breach in India has left a billion people at risk of identity theft," Washington Post, January 4, 2018, www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/.

[83] 2017: Poor Internal Security Practices Take a Toll," The Breach Level Index (Gemalto, 2017), breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

[84] Niall McCarthy, "The Average Cost Of A Data Breach Is Highest In The U.S.[Infographic]," Forbes, July 13, 2018, www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#1b55d30c2f37

[85] "Vodafone Group FAQs on Privacy and Security," (Vodafone Group, December 2017), www.vodafone.com/content/dam/vodafone-images/sustainability/downloads/VodafoneGroupFAQsonPrivacyandSecurity_December2017.pdf.

[86] "Information Security Technology - Personal Information Security Specification" (Standardization Administration of China, May 2018), www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf.

[87] See Articles 33 and 34 of "Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)" (European Parliament and European Council, April 27, 2016), eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

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

[89] "Australia data encryption laws explained," BBC News, December 7, 2018, www.bbc.com/news/world-australia-46463029.

[90] Siobhan Conners, "What is the Investigatory Powers Act 2016?," IT PRO, April 10, 2019, www.itpro.co.uk/policy-legislation/33407/what-is-the-investigatory-powers-act-2016.

[91] Yuan Yang, "China's cyber security law rattles multinationals," Financial Times, May 30, 2017, www.ft.com/content/b302269c-44ff-11e7-8519-9f94ee97d996.

[92] Ramsha Jahangir, "UN expert urges countries to protect right to privacy in digital age," DAWN, September 11, 2018, www.dawn.com/news/1432243.

[93] Kurt Wagner, "WhatsApp is at risk in India. So are free speech and encryption," Recode, February 11, 2019, www.recode.net/2019/2/19/18224084/india-intermediary-guidelines-laws-free-speech-encryption-whatsapp.

[94] See the 2019 RDR Index methodology at: rankingdigitalrights.org/2019-indicators/#P16.

[95] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (European Union, April 5, 2016), eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[96] "Information Security Technology – Personal Information Security Specification (GB/T 35273-2017)" (Standardization Administration of China, May 2018), std.sacinfo.org.cn/gnoc/queryInfo?id=5765F72B812F670F1571443FF09C12D2.

[97] "The Personal Data Protection Bill, 2018" (Ministry of Electronics and Information Technology, July 27, 2018). meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

[98] "Protection of Personal Information Act, 2013 (Act No. 4 of 2013): Regulations Relating to the Protection of Personal Information (Department of Justice and Constitutional Development, December 14, 2018), www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister.pdf.

[99] "Proposal for an ePrivacy Regulation" (European Commission, January 2017), ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[100] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (European Union, April 5, 2016), eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[101] "Information Security Technology – Personal Information Security Specification (GB/T 35273-2017)" (Standardization Administration of China, May 2018).

[102] "2016 Cybersecurity Law" (Standing Committee of the National People's Congress, November 7, 2016), www.chinalawtranslate.com/en/cybersecuritylaw/.

[103] "The Personal Data Protection Bill, 2018" (Ministry of Electronics and Information Technology, July 27, 2018).

[104] "Recommendations on Privacy, Security, and Ownership of the Data in the Telecom Sector" (Telecom Regulatory Authority of India, July 16, 2018), main.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf.

[105] Protection of Personal Information Act, 2013 (Act No. 4 of 2013): Regulations Relating to the Protection of Personal Information (Department of Justice and Constitutional Development, December 14, 2018).

[106] "Assembly Bill No. 375 Chapter 55: An Act to Add Title 1.81.5 (Commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, Relating to Privacy, Also Known as California Consumer Privacy Act of 2018 ('CCPA')" (California Legislature, June 29, 2018), leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[107] See Articles 5(1)(a) and the information obligations in Articles 12, 13, and 14 of the "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (European Union, April 5, 2016).

[108] See Articles 33 and 34 of the "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (European Union, April 5, 2016).

[109] According to Articles 2(2)(d) the processing of personal data by authorities for the purposes of crime prevention, investigations, and safeguarding public security are not within the scope of the GDPR. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (European Union, April 5, 2016).

[110] "The GNI Principles," Global Network Initiative, accessed April 23, 2019, globalnetworkinitiative.org/gni-principles/.

[111] "Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)" (European Commission, October 1, 2017), eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[112] "Access Now's comments to the proposed e-Privacy Regulation" (Access Now, June 2017), www.accessnow.org/cms/assets/uploads/2017/06/ePrivacy-paper-amendments-Access-Now.pdf

[113] "International Principles on the Application of Human Rights to Communications Surveillance" (Necessary and Proportionate, May 2014), necessaryandproportionate.org/principles.

[114] See the 2019 RDR Index methodology at: rankingdigitalrights.org/2019-indicators/.

[115] Figures as of March 25, 2019. "World Internet Users and 2019 Population Stats," Internet World Stats, accessed April 22, 2019, www.internetworldstats.com/stats.htm.