RANKING DIGITAL RIGHTS
Winter 2020 Investor Update

Digital rights 2020 outlook: Market realities and regulation are raising the bar

Rebecca MacKinnon
Director, Ranking Digital Rights

Melissa Brown
Partner, Daobridge Capital Limited; Advisor, Ranking Digital Rights

Jasmine Arooni
2019 Policy and Legal Intern, Ranking Digital Rights

About the RDR Investor Update

This third edition of the RDR Investor Update draws on the findings of the 2019 RDR Corporate Accountability Index to offer institutional investors insights into key human rights risks of the world's most important internet, mobile, and telecommunications companies.

To read the 2019 RDR Index, visit rankingdigitalrights.org/index2019.

Contents

At a time of regulatory and geopolitical uncertainty, investors should look for tech companies that understand how human rights standards build trust. Several companies have made notable improvements since the first RDR Corporate Accountability Index started evaluating many of the world's most important internet, mobile, and telecommunications companies in 2015. Most of the industry, however, has focused on legal compliance and lobbying to shape further regulation. Companies otherwise have done little to be proactive in response to widespread public concerns about their social impact.

They continue to expose users and investors to risk by failing to disclose adequately what happens to users' data or how they can control its collection and use. Companies do not disclose enough information about who has the power to amplify online messages and under what circumstances, or about how online speech and access to or about information are enabled, restricted, and shaped through digital platforms, services, and devices. The RDR Index offers investors a clear framework to evaluate how companies can prevent or mitigate risks to users' privacy, expression, and information rights, in alignment with the UN Guiding Principles for Business and Human Rights.

Look for companies with policies, practices, and governance that go above and beyond legal compliance box-checking. Despite significant shortcomings in policy, practice, and disclosure, some progress has been made. The highest-ranked tech companies in the 2019 RDR Index disclosed policies and practices that exceeded baseline privacy and internet-related laws and regulations in their relevant jurisdictions, thereby meeting higher human rights standards in at least some areas. One sign that regulatory drivers can reshape behavior came with the General Data Protection Regulation (GDPR). After the regulation came into force in May 2018, companies improved, albeit unevenly. The quality of privacy and security policies, practices, and disclosures by EU-based telcos varied widely in the 2019 RDR Index. For example, **Deutsche Telekom** (the highest ranking European telco) out-scored **Orange** (the lowest-ranking European telco) by nearly double in the privacy category. For more detail and examples, see p. 5.

CEOs and boards need to take responsibility for the human rights risks and negative social impacts associated with their business models. The 2019 RDR Index evaluated whether companies carry out comprehensive due diligence addressing the full range of risks to internet users and affected communities associated with their business operations. No companies disclosed any evidence that they conduct due diligence or human rights impact assessments in connection with targeted advertising business models. This performance gap is striking at a time when widespread media reports backed by academic research show that personal data shared by companies with advertisers can be abused to target specific groups of people with discriminatory practices or with blatant disinformation that can incite violence or sway political outcomes.

Investors need to focus on governance issues that affect how dominant social media platforms' content rules are formulated and enforced as well as how algorithms and artificial intelligence are used to shape content or profile users. These issues matter because **Facebook**, **Twitter**, and Alphabet's **Google** (parent of YouTube) have not offered any evidence of having conducted human rights impact assessments on their rules, content policing processes, or their use of algorithms, machine learning, or other artificial intelligence tools. For more detail and examples, see p. 7.

About the RDR Corporate Accountability Index

Published in May 2019, the Ranking Digital Rights 2019 Corporate Accountability Index evaluates 24 of the world's most important internet, mobile, and telecommunications companies on their publicly disclosed commitments, policies, and practices affecting freedom of expression and privacy.

For in-depth analysis, company report cards, and a downloadable report, see rankingdigitalrights.org/index2019.

For previous editions of RDR investor briefs and other resources, see rankingdigitalrights.org/investors.

The next RDR Index will be released in early 2021 following a period of research, pilot testing, and stakeholder consultation to add new indicators addressing human rights risks of automation and machine learning as well as targeted advertising business models. At least two new companies will be added: Amazon and Alibaba.

The RDR Index uses standards to evaluate companies, drawing on more than a decade of work by the human rights, privacy, and internet security communities. These standards include the UN Guiding Principles on Business and Human Rights, which affirm that while 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 principles 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. 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 investors, and are used by companies to improve their own policies.

Research approach

RDR's methodology focuses on how ICT sector companies' policies and commitments related to their core business operations affect users' freedom of expression and privacy, both of which are universally recognized human rights. This framing is crucial for internet and telecom leaders that must address strategic issues at a global scale.

The 2019 RDR Index evaluates companies' publicly disclosed commitments and policies relating to corporate practices across 35 indicators divided into three distinct categories:

Governance: board and corporate-level oversight, internal accountability mechanisms, risk assessment, and grievance mechanisms;

Freedom of Expression: how companies manage or restrict information published or transmitted through their platforms, either due to regulatory demands or commercial incentives;

Privacy: company disclosures about the management and commercial use of all information that could be used to identify or profile a user, handling of government demands for user information, and measures in place to secure user information.

The 24 companies assessed in the 2019 RDR Index were selected because their products and services are collectively used by more than half of the world's fixed line and mobile internet users. Thus, while the results are not fully comprehensive, and RDR does not assess performance and impact of specific policies and commitments, they nonetheless point to the most important global risks.

Learn more about the RDR Index

- Subscribe to our newsletter, The Radar: rankingdigitalrights.org/newsletter
- Full set of 2019 RDR Index indicators: rankingdigitalrights.org/2019-indicators
- Company results by indicator: rankingdigitalrights.org/index2019/indicators
- Full dataset and printable PDF: rankingdigitalrights.org/index2019/download

Institutional investors: Please take our survey and help us meet your needs.

Do you hold shares in major listed internet, mobile, and telecommunications companies? If so, please take our investor survey to help Ranking Digital Rights better understand how investors use the RDR Index and its related resources, such as the Investor Update. www.surveymonkey.com/r/RDR2019

Growing shareholder concern for digital rights

For investors and other stakeholders tracking the evolution of digital rights issues, stewardship initiatives offer useful insights. The number of shareholder resolutions on issues related to digital rights has jumped from 2 in 2015, to 3 in both 2016 and 2017, to 4 in 2018, to 12 in 2019 (see table below).

While none of the following shareholder resolutions came close to passing, they reflect a growing concern about the business impacts of tech companies' failures to adequately understand and mitigate digital rights risks. A strong theme across many of the proposals that made it onto proxy ballots in 2019 is the need for more responsible and accountable governance – particularly in relation to online speech, artificial intelligence, and business models, in addition to long-standing privacy concerns.

The increase in digital rights-related shareholder resolutions also reflects increased coordination and organization among responsible investors, driven in part by the Investor Alliance for Human Rights, which has recently chosen to make digital rights issues a priority focus.[1] The outlook for 2020 and beyond will depend on two key factors: whether companies are able to convince shareholders to withdraw some proposals by responding satisfactorily to concerns, and whether the SEC succeeds in increasing the thresholds of shareholder support required for inclusion in proxy materials.[2]

Proxy ballots in 2019 reflected an increasing need for more responsible and accountable governance.

Notable digital rights-related shareholder resolutions in 2019

The table below lists major technology companies and the shareholder resolutions proposed for each during 2019, along with the applicable RDR Index indicators (right-hand column), which are listed on p. 11. You can also find an interactive table—updated as new resolutions are proposed—with links to the resolutions and the relevant indicators at rankingdigitalrights.org/shareholder-resolutions.

Company	Shareholder resolution	Related RDR Index indicators
Alphabet/ Google	Report on Content Governance	G4, G6, F3, F4, F8
	Report on Human Rights Assessment of Google Search in China	G4, G6, F3, F5, F6, F8, P10, P11, P12
	Define Strategic Alternatives to Maximize Shareholder Value (regarding company size and structure)	G2, G4, G5, G6, F5, F6, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12, P15
	Establish a Societal Risk Oversight Committee	G2, G4, G5, G6
Amazon	Prohibit the Sale of Facial Recognition Technology to Government Agencies	G5, G6, P10, P11
	Report on the Impact of Facial Recognition Technology on Civil Rights	G2, G4, G5, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12
	Report on Efforts to Address Hate Speech and Sale of Offensive Products	G4, G5, F1, F3, F4
Facebook	Retain Advisors to Study Strategic Alternatives (regarding company size, structure, and business model)	G2, G4, G5
	Report on Content Governance Policies	G1, G2, G4, G6, F1, F3, F4, F5, F6, F8, P10, P11, P12
Twitter	Report on Content Enforcement Policies	G2, G4, G6, F1, F3, F4, F8
Verizon Media	Address Cybersecurity and Data Privacy	G2, G4, F1, F3, F5, F7
	Address Child Sexual Exploitation	P13, P14, P15, F16, P17, P18

Even after the GDPR was implemented, privacy scores varied widely for EU companies.

Privacy: Leading indicators

A growing number of complaints against companies for GDPR violations are working their way through European courts and more privacy legislation is in the cards for 2020 in Europe.[3] In the U.S., the California Consumer Privacy Act took effect in January 2020. Though the timeline for the passage of national legislation is unclear, several bills have been introduced in the U.S. Congress.[4] Rather than simply looking for compliance preparation, investors may want to focus on companies that take proactive measures to demonstrate good data stewardship, whether or not the law compels them to do so.

As mentioned on the first page of this Investor Update, despite the fact that the 2019 RDR Index research cycle started after the GDPR went into force in the EU in May 2018, our privacy scores of EU-based companies varied widely, as Figure 1 illustrates.[5] It should be noted that the RDR Index evaluates a much wider range of privacy-related issues than the GDPR addresses. In many cases where RDR indicators and GDPR overlap in addressing a specific practice pertaining to the collection and sharing of user information, RDR sets a higher or more specific disclosure standard. Therefore, RDR's privacy scores do not reflect a company's GDPR compliance.

Companies that rank highest on privacy in the RDR Index have gone above and beyond the letter of regulatory compliance. This finding means that high-scoring companies are better prepared for the next wave of privacy regulation. Beyond this, by maximizing respect for users' privacy as a human right through strong disclosures and responsible

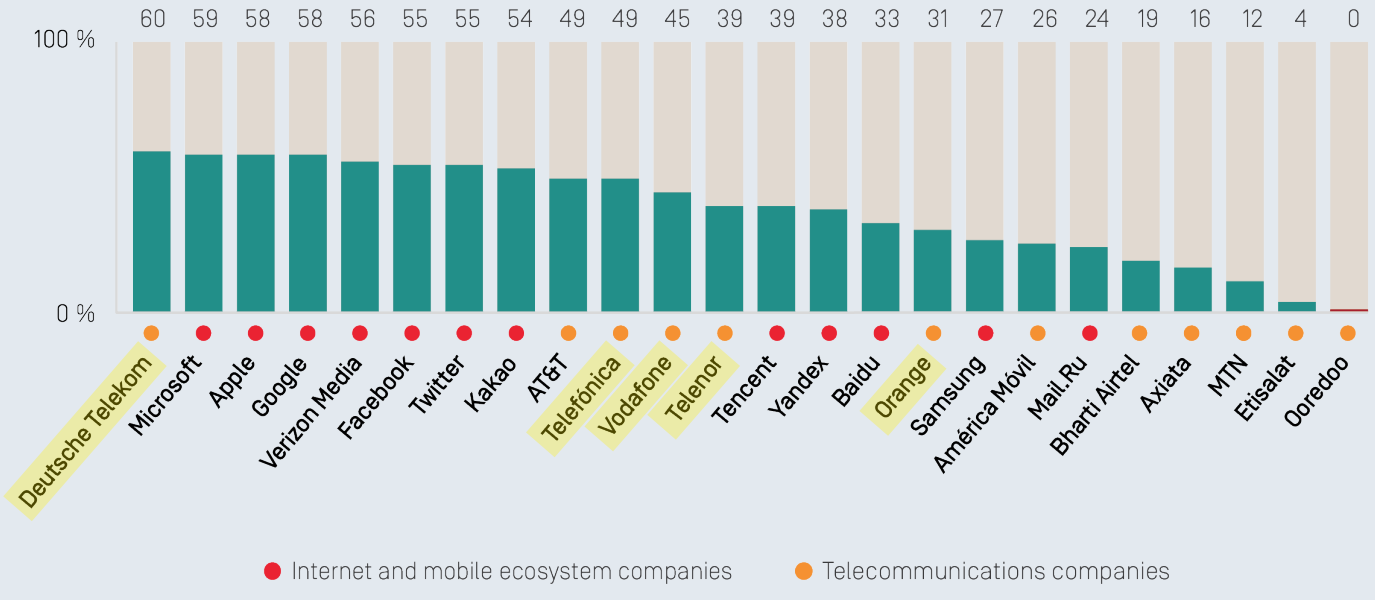
Figure 1: How transparent are companies about policies and practices affecting users' privacy and security?

The table below shows 2019 RDR Index company scores in the privacy category. EU-based telecommunications companies are highlighted in yellow.

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. For a full list of indicators, see p. 11 or review the privacy indicators at rankingdigitalrights.org/2019-indicators/#P

Indicators assess:

1. Accessibility and clarity of privacy policies;
2. How transparent companies are about how they collect, share, and handle user information;
3. How companies handle government and other types of third-party requests for user information;
4. If companies have clear processes and safeguards in place for keeping user information secure.



practices, these companies are mitigating harms that befall users as a result of poor data stewardship, regardless of legality.

By examining company performance on specific RDR Index indicators, investors can gain a more granular picture of specific types of risk. For example, Figure 2 illustrates the score breakdown for one indicator (P7) that examines whether companies clearly disclose the options users have to control how their information is used and shared. The highest score for that indicator, 63 percent, was earned by the German telecommunications company **Deutsche Telekom**, while **Orange** of France earned only 6 percent, and Spain's **Telefónica** and **Vodafone** of the UK also earned poor grades.[6]

Companies that rank highest on privacy in the RDR Index have gone above and beyond the letter of regulatory compliance.

Online speech: Proactive transparency about content enforcement

The media is awash with headlines about online extremism, hate speech, and disinformation. Debates about appropriate regulatory responses—from increasing intermediary liability to antitrust—make it harder to predict the regulatory future for online speech than for privacy.

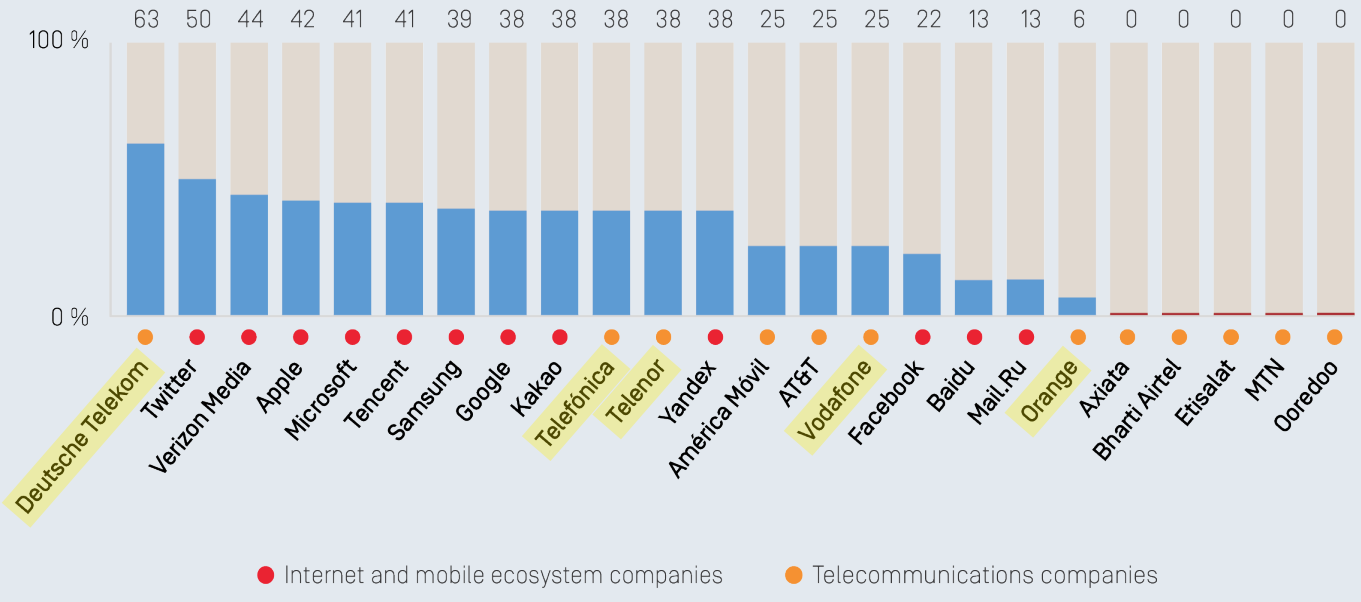
Under such circumstances, look for efforts by companies to be accountable to users and affected communities despite the absence of clear regulation. A key first step will be for companies to be more transparent about how they formulate and enforce rules for paid as well as organic user content. Greater disclosure will contribute to a more informed policy discussion about what types of rules would be most appropriate.

Figure 2: The company should disclose to users what options they have to control how their information is collected, used, retained, and shared (Indicator P7)[7]

The table below represents company scores in the 2019 RDR Index Privacy category. EU-based telecommunications companies are highlighted in yellow.

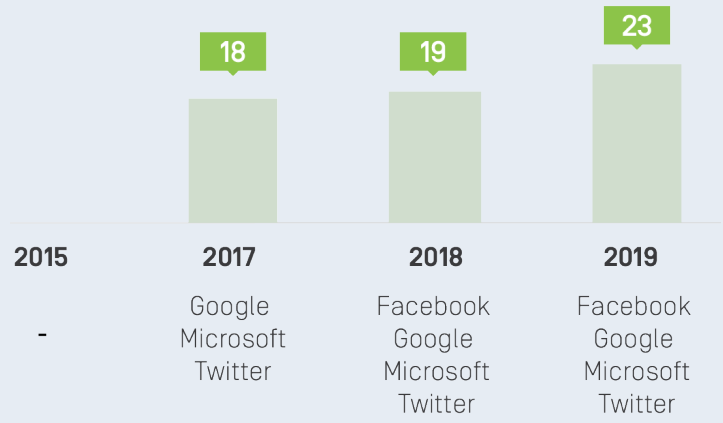
To assess adequate disclosure by companies, Indicator P7 considers:

1. Whether users have options to control what is collected;
2. Whether that information can be deleted;
3. Whether users have options to control how their information is used for targeted advertising;
4. Whether targeted advertising is off by default (in other words, users must opt-in to receive ads, rather than having to opt-out to avoid them);
5. Whether users can control a device's geolocation functions (for mobile ecosystems only).



Look for proactive efforts by companies to be accountable to users and affected communities despite the absence of clear regulation.

Figure 3: The company should disclose data about how it enforces terms of service (Indicator F4)[12]



Indicator F4 in the Freedom of Expression category of the 2019 RDR Index 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. As the graph above shows, since the first 2015 RDR Index, when no companies disclosed anything, progress has been made by a few companies, but disclosure still falls short.

For example, every company should clearly disclose and regularly publish data about the volume and nature of actions they take to restrict content or accounts that violate the company's rules. Since its inception, the RDR Index has measured whether companies disclose any such data. Figure 3 shows average scores for this indicator since the inaugural 2015 RDR Index, when no companies published any data about content they had removed to enforce their terms of service.

While most companies still fail to publish any data about actions they are taking to enforce terms of service and community standards, four companies have improved their disclosure over the past four years.[8] To varying degrees **Facebook**, **Google**, **Microsoft**, and **Twitter** have steadily been releasing more granular and detailed information about the volume and nature of content removed, and accounts deactivated, in the course of enforcing their respective terms of service.

Scores for these four companies are expected to rise further on this indicator in future iterations of the RDR Index. In November 2019, for example, **Facebook** published a new transparency report containing more detailed data on questions such as how widely content was viewed before being taken down and how much content was restored after appeal. It also included information about its subsidiary Instagram's content enforcement for the first time.[9] In light of regulatory threats in Europe around hate speech and disinformation, such increased transparency is a necessary proactive move.

Governance: The importance of human rights impact assessments

As governments rush to set new rules for how platforms should address illegal or problematic speech, RDR's findings highlight a glaring absence of basic corporate governance, oversight, and mitigation of risks related to the management and policing of online content. Few companies evaluated in the 2019 RDR Index showed any evidence of due diligence around how their design choices, business models, rule-setting processes, and deployment of automation could contribute to the spread of harmful content.

A strategy of challenging the governance of companies has the potential to drive positive performance improvements. While debates about regulation of digital platforms usually focus heavily on who should be held responsible for identifying and removing different types of online speech, there has been insufficient focus on companies' upstream

governance and policy decisions that have failed to prevent the downstream deluge of content-related problems. To improve their ability to anticipate and address downstream harms caused by disinformation campaigns, violent extremism, and other forms of speech that dominate news coverage, companies must strengthen their governance and policy frameworks.

Investors have good reason to be concerned about the lack of evidence of such frameworks as of 2019. Indicator G4 in the Governance category of the 2019 RDR Index is based on the principle that companies should conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify and mitigate risks of all aspects of their business activities on freedom of expression and privacy.[10]

As of 2019, most companies that show any evidence of conducting human rights due diligence have limited those efforts to focus on human rights harms associated with government censorship and surveillance demands. As shown in Figure 4, companies scoring 70 or above on human rights due diligence are all members of the Global Network Initiative (GNI), whose members commit to conduct human rights impact assessments in relation to government censorship requests and demands for user data that they receive from around the world.

The highest-scoring companies on this indicator went above and beyond the due diligence scope required of GNI members to include aspects of their business operations not directly related to government demands.

Three specific elements of Indicator G4 consider whether companies disclosed any evidence that they conduct human rights impact assessments of the following practices:

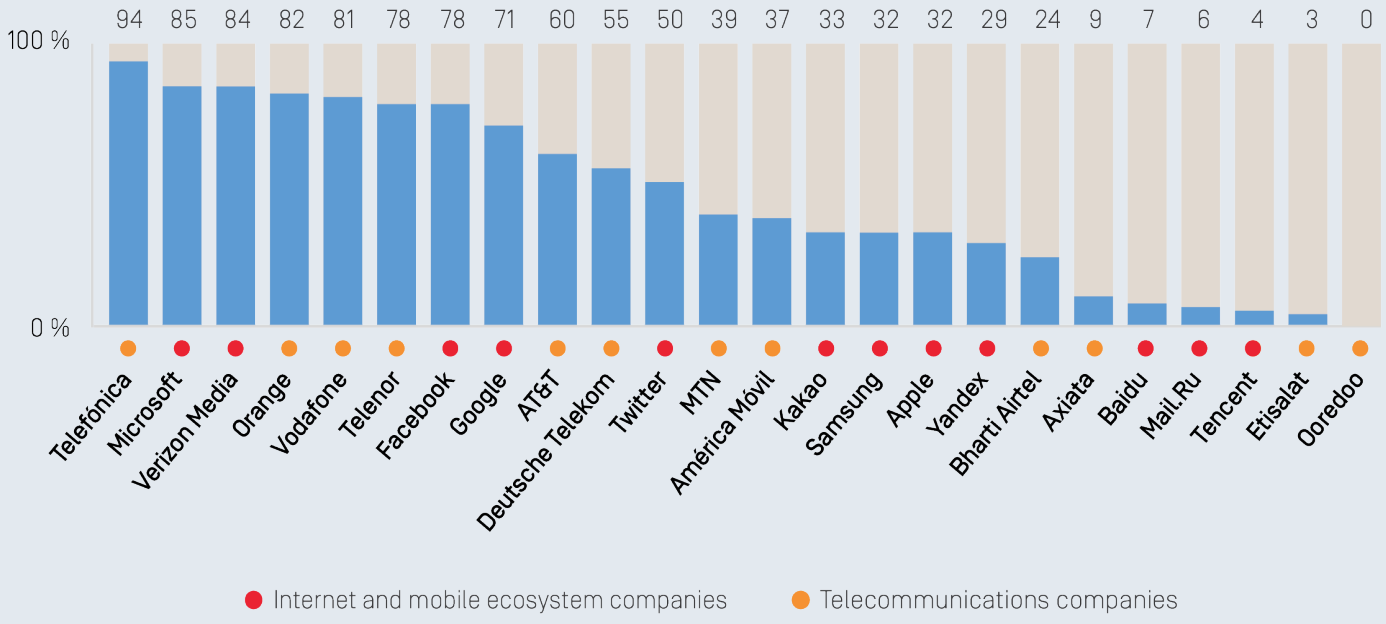
- Enforcing of their terms of service;
- Using algorithms, automated decision making, and artificial intelligence;
- Allowing marketers and advertisers to target specific users with select messages.

RDR's findings highlight a glaring absence of basic corporate governance, oversight, and mitigation of risks related to online content.

Figure 4: The company should conduct comprehensive human rights impact assessments (Indicator G4)

The graph below shows 2019 RDR Index scores for Indicator G4, which 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.

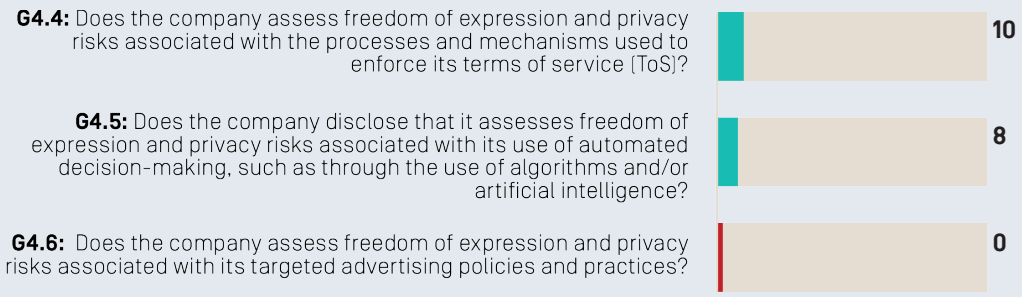
For a full list of indicators, see p. 11, or review the guidance for Indicator G4 at rankingdigitalrights.org/2019-indicators/#G4.



This approach provides an important lens for identifying which companies are taking systematic steps to address the human rights risks of their business models, which are heavily supported by targeted ads and artificial intelligence tools. As shown in Figure 5, only four companies out of the 24 evaluated in the 2019 RDR Index disclosed any such due diligence. Notably **Facebook**, **Twitter**, and Alphabet's **Google** (parent of YouTube) were among those found to conduct no human rights due diligence in these areas. Yet all three have come under fire for the ways in which their targeted advertising practices are used to spread disinformation, how their rules about permissible content are developed and enforced, and how their algorithms contribute to the viral spread of violent extremism.[11]

Figure 5: Three specific elements of human rights impact assessments (Indicator G4)

For the 2019 RDR Index, Indicator G4 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 of their automated decision-making tools (such as algorithms and artificial intelligence), or of their targeted advertising policies and practices. The graph below shows the sub-scores for three specific elements of Indicator G4. Total scores for these companies appear in Figure 4, on p. 7.



Burning issues in 2020: Algorithms, targeted ads, and the threat of disinformation to democracy

While the spotlight on the world's most powerful tech giants is already strong, scrutiny of how their operations affect the public interest will only intensify in a highly volatile U.S. election year. Under such circumstances, corporate responsibility and accountability around advertising business models and use of algorithmic decision-making systems becomes even more important. Why? Companies that derive revenue from targeted advertising collect and process vast amounts of personal data. Doing so enables them to manage, shape, and govern the flow of content and information on their platforms in a way that maximizes advertising revenue. They are able to do so with the assistance of algorithmic decision-making systems.

The use of these systems can pose risks to users' rights to free expression, access to information, and privacy. The systems can amplify, prioritize, and shape content according to data- and machine-driven inferences about a user's preferences or personal traits. Information systems that prioritize content based on popularity are vulnerable to disinformation campaigns, hate speech, and other harmful content, which can unfairly influence public opinion, undermine democratic processes, and lead to real-life harm. RDR has piloted a set of draft indicators, including questions such as those listed on the next page, that will be integrated into the methodology for the fifth RDR Index.

Scrutiny of how tech giants' operations affect the public interest will only intensify in a highly volatile U.S. election year.

The next RDR Index

In 2020 the RDR research team will expand the methodology for the RDR Corporate Accountability Index to address human rights harms associated with targeted advertising, algorithms, and machine learning. We will also adapt the methodology to include more company types, especially powerful global platforms with core e-commerce businesses, such as Amazon and Alibaba. The 2020 RDR Index will be published in early 2021 with the expanded methodology and scope.

Questions for investors to ask about targeted advertising and algorithmic systems

In 2019, RDR developed and piloted a set of draft indicators through a rigorous research and consultation process. Pilot results will be published in February 2020. These indicators, captured in the questions below, will offer researchers and investors an early look at the best way to monitor corporate performance on some of the tech sector's highest risk practices. After further stakeholder consultation, they will be revised and integrated into the methodology for the fifth RDR Index, which will be released in early 2021.

The full set of draft indicators with explanations and definitions can be downloaded at rankingdigitalrights.org/2019/10/18/newindicators.

Questions for investors to ask about these risks:

Does the company conduct human rights impact assessments on processes for policy enforcement, targeted advertising, and algorithmic decision-making systems?

For targeted advertising, does the company clearly disclose:

- Its policies for what advertising content is prohibited?
- How advertisers can target users through its platform or service, what targeting parameters are available to advertisers, and whether there are categories of users that advertisers are prohibited from targeting?
- How users can access key information about the targeted advertising that they see?
- Whether targeted advertising is on or off by default?

For algorithmic decision-making systems, does the company clearly disclose:

- Policies outlining practices involving the use of algorithmic decision-making systems?
- How online content is curated, ranked, or recommended?
- Whether users are given options to control how the content they see is curated, ranked, or recommended?
- Whether users' information is used to develop algorithmic systems?

For automated software agents or "bots," does the company clearly disclose:

- If it has clear rules around whether bots are permitted on a platform or service and what rules they must conform to?
- If it requires bots to be clearly labeled as such?
- How it enforces its policies related to bots?

Key questions for investors to ask companies

While the questions on the previous page cover emerging issues, the following 12 categories of questions offer 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 published as part of the 2019 RDR Index.[13]

1. **Oversight:** Does the board of directors exercise direct oversight over risks related to user security, privacy, and freedom of expression? Does board membership include people with expertise and experience on issues related to digital rights? (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 with regard to 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(s), 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 making security updates available 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)

2019 RDR Index indicators

The 2019 RDR Corporate Accountability Index ranks 24 companies according to 35 indicators evaluating company disclosure of policies and practices affecting governance, freedom of expression, and privacy. For more information about the indicators, visit rankingdigitalrights.org/index2019/indicators.

G: Governance

G1. Policy commitment

G2. Governance and management oversight

G3. Internal implementation

G4. Impact assessment

G5. Stakeholder engagement

G6. Remedy

F: Freedom of Expression

F1. Access to terms of service

F2. Changes to terms of service

F3. Process for terms of service enforcement

F4. Data about terms of service enforcement

F5. Process for responding to third-party requests for content or account restriction

F6. Data about government requests for content or account restriction

F7. Data about private requests for content or account restriction

F8. User notification about content and account restriction

F9. Network management (telecommunications companies)

F10. Network shutdown (telecommunications companies)

F11. Identity policy

P: Privacy

P1. Access to privacy policies

P2. Changes to privacy policies

P3. Collection of user information

P4. Sharing of user information

P5. Purpose for collecting and sharing user information

P6. Retention of user information

P7. Users' control over their own user information

P8. Users' access to their own user information

P9. Collection of user information from third parties (internet companies)

P10. Process for responding to third-party requests for user information

P11. Data about third-party requests for user information

P12. User notification about third-party requests for user information

P13. Security oversight

P14. Addressing security vulnerabilities

P15. Data breaches

P16. Encryption of user communication and private content

P17. Account security (internet, software, and device companies)

P18. Inform and educate users about potential risks

References

1. Siobhan Riding, "Digital human rights are next frontier for fund groups," *Financial Times*, November 10, 2019, www.ft.com/content/0866d79f-cd48-42d4-b21c-453f964d2fb0
2. Ganesh Setty, "Shareholders would have tougher time submitting resolutions under SEC's proposed rule," *CNBC*, November 5, 2019, www.cnbc.com/2019/11/05/rule-change-would-make-it-harder-to-submit-shareholder-resolutions.html
3. Jessica Davies, "Everything you need to know about Europe's data privacy regulations," *Digiday*, October 25, 2019, digiday.com/uk/all-you-need-to-know-about-europes-data-privacy-regulations
4. Matt Laslo, "Should tech CEOs go to jail over data misuse? Some senators say yes," *Wired*, October 30, 2019, www.wired.com/story/wyden-mind-your-own-business-act
5. "2019 RDR Corporate Accountability Index – Privacy," *Ranking Digital Rights*, May 2019, rankingdigitalrights.org/index2019/report/privacy
6. All Ranking Digital Rights indicators are referenced using a letter denoting their category (e.g. P for privacy, G for governance) and a number. A complete list of 2019 indicators can be found here: rankingdigitalrights.org/2019-indicators
7. "2019 RDR Corporate Accountability Index – Privacy: Section 53," *Ranking Digital Rights*, May 2019, rankingdigitalrights.org/index2019/report/privacy
8. "2019 RDR Corporate Accountability Index – Freedom of Expression: Section 42," *Ranking Digital Rights*, May 2019, rankingdigitalrights.org/index2019/report/privacy
9. Guy Rosen, "Community Standards Enforcement Report, November 2019 Edition," *Facebook*, November 13, 2019, www.about.fb.com/news/2019/11/community-standards-enforcement-report-nov-2019
10. 2019 Indicators – G4. Impact assessment," *Ranking Digital Rights*, May 2019, rankingdigitalrights.org/index2019/report/privacy
11. "Surveillance giants: How the business model of Google and Facebook threatens human rights," *Amnesty International*, November 21, 2019, www.amnesty.org/en/documents/pol30/1404/2019/en

    Louise Matsakis, "Facebook's ad system might be hard-coded for discrimination," *Wired*, April 6, 2018, www.wired.com/story/facebooks-ad-system-discrimination

    Emma Ellis, "The alt-right are savvy internet users. Stop letting them surprise you," *Wired*, September 19, 2018, www.wired.com/story/alt-right-youtube-savvy-data-and-society
12. 2019 Indicators – G4. Impact assessment," *Ranking Digital Rights*, May 2019, rankingdigitalrights.org/index2019/report/privacy
13. "2019 RDR Index – Companies," *Ranking Digital Rights*, May 2019, rankingdigitalrights.org/index2019/report/privacy

About Ranking Digital Rights

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

- For more about Ranking Digital Rights and the Corporate Accountability Index, visit rankingdigitalrights.org.
- For more about New America, visit www.newamerica.org.
- For more about the Open Technology Institute, visit www.newamerica.org/oti.

About the authors

Melissa Brown is a partner at Daobridge Capital, a Hong Kong–based investment advisory firm. Over the past 15 years, she has been actively involved in a range of innovative initiatives focused on Asian listed companies, sustainable investment, and corporate governance.

Rebecca MacKinnon directs the Ranking Digital Rights project at New America. Author of *Consent of the Networked: The Worldwide Struggle For Internet Freedom*, she is co-founder of the citizen media network Global Voices and a former CNN bureau chief and correspondent in Beijing and Tokyo.

Jasmine Arooni is a J.D. candidate at the George Washington University Law School, where she focuses on internet, privacy, and cybersecurity law. She worked in cybersecurity program management at Sony prior to law school and spent the past summer as a legal and policy intern at Ranking Digital Rights working on privacy and investor relations.