Introduction

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

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

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

If human rights are to be protected and respected around the world, the internet must be designed, operated, and governed in a way that reinforces the protection and exercise of human rights. That is not presently the case. The Ranking Digital Rights 2018 Corporate Accountability Index offers detailed evidence as to exactly *how* the world's most powerful internet, mobile, and telecommunications companies are failing to respect users' rights. Too few companies make users' rights a central priority

for corporate oversight, governance, and risk assessment. Most withhold even basic information about measures they take to keep users' data secure. None disclose enough about how personal information is handled, including what is collected and shared, with whom, and under what circumstances. They are all much too opaque about how content and information flows are policed and shaped through their platforms and services.

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

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

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

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

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

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

Beyond 2018: As technology and geopolitics evolve, we will continue to re-evaluate and adapt our methodology. In the second half of 2018, we hope to conduct research and consultations to determine

what indicators may need to be added to address the need for corporate transparency around the deployment of algorithms and artificial intelligence, and how targeted advertising technologies affect users' rights. As always, we will report on progress and invite feedback on our website at: https://rankingdigitalrights.org.

Footnotes

---

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

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

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

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

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