Poor Digital Rights Governance:
Users, Investors, and Societies Pay the Price

OCTOBER 29, 2018

Rebecca MacKinnon
Director, Ranking Digital Rights

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

Lessons from 2018's crash course on digital rights and a watch list for 2019

Last year's 2017 Investor Research Note identified concrete risks stemming from how companies manage user data and content. Poor disclosure of inadequate policies by internet, mobile, and telecommunications companies covering online expression, privacy, and security topped the list of red flags.

In 2018 these issues and risks have become more demonstrably material. This year's Investor Update reviews key developments of 2018 and their relationship to the Ranking Digital Rights Corporate Accountability Index findings and methodology.

CONTENTS

The Ranking Digital Rights (RDR) 2018 Corporate Accountability Index findings foreshadowed many of the corporate governance and disclosure problems reflected in this year's negative news headlines. While industry leaders play catch up on a growing list of digital rights risks, RDR's research process continues to identify new trouble spots. RDR provides the data, information, and tools needed to understand the regulatory and legal trade-offs that will influence future investment outcomes, and can help to inform investors' engagement strategies.

2018 taught us that good corporate governance now requires broader understanding of material risks in the information communications and technology (ICT) sector. Until recently, risk assessments in the sector have generally focused on regulatory compliance and technical security. However, recent events have shown that "cyber security" and "cyber risk" have been too narrowly focused on criminal and espionage activities: data breaches, break-ins, and theft of user data or proprietary commercial information. Then came the news in early 2018 that Facebook had exposed the data of as many as 87 million users to the political consulting firm Cambridge Analytica. In the spring of 2018, activists in Myanmar were warning that social media was aiding genocide in their country. These and other events of the past year have underscored the need for companies to wake up to consumer privacy and expression-related risks.

Even if a hacker does not steal people's data, flawed business models designed to obscure the true price users pay—by giving companies access to their private information, communications, and financial transactions—need to be re-assessed urgently. Public trust is breached when personal information ends up being used by political operatives or repressive regimes seeking to undermine the democratic process or target advocates and journalists. It is also breached when platforms fail to manage content and information flows in a transparent and accountable manner that respects the expression rights of vulnerable minorities, demonstrators, and investigative journalists while also stopping those seeking to use their platforms and services to plan and incite violence.

How should corporate boards exercise responsible oversight over these digital rights risks? The focus should be on oversight of how business models affect users' rights, including privacy and expression. At a minimum, better governance must start with tangible improvements in company disclosure of policies and practices affecting both privacy and how companies manage and police online speech and content. Users with concerns about how their data was shared, or about restrictions of content or accounts, should have access to effective grievance and remedy mechanisms. Companies should carry out regular and rigorous impact assessments on all aspects of the business that might either cause or facilitate harm to users—individually or collectively. Companies that fail to act as responsible stewards of personal data and public discourse can expect a regulatory backlash that may or may not result in constructive solutions. Investors should reward those that address their risks, working with stakeholders to devise innovative solutions that enable the internet to realize its early promise as an enabler of global connectivity and innovation as well as democracy and human rights.

About the Corporate Accountability Index

Published in April 2018, the **Ranking Digital Rights 2018 Corporate Accountability Index** evaluates 22 of the world's most important internet, mobile, and telecommunications companies on disclosed commitments, policies, and practices affecting freedom of expression and privacy. For in-depth analysis and data as well as a downloadable report and company report cards please visit https://rankingdigitalrights.org/index2018. The next Index will be released in May 2019.

For the 2017 Investor Research Note and other resources see: https://rankingdigitalrights.org/investors/

The standards the Index uses to evaluate companies build on more than a decade of work by the human rights, privacy, and security communities. These standards include the 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 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 Index further draws on a body of emerging global standards and norms around data protection, security, and access to information.

The Index data and analysis inform the work of human rights advocates, policymakers, and 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 in an international context.

RDR 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 22 companies assessed 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.

2018 Index materials:

Full set of 2018 Index indicators: https://rankingdigitalrights.org/2018-indicators/

Company results by indicator: https://rankingdigitalrights.org/index2018/indicators/

Full dataset and printable PDF: https://rankingdigitalrights.org/index2018/download/

2019 Index materials:

Full set of 2019 Index indicators: https://rankingdigitalrights.org/2019-indicators/

List of 2019 companies and services: https://rankingdigitalrights.org/2019-companies/

Poor disclosures were red flags signaling companies' failure to anticipate and mitigate risks to freedom of expression and privacy.

2018 Governance Lessons

Poor disclosures—especially when signaling an underlying lack of adequate governance practices—were red flags that predicted companies' failure to anticipate and mitigate risks to users' expression and privacy rights that have turned out to be costly for companies in 2018 and beyond.

Board- and Executive-Level Oversight

Google's relatively poor showing in the Governance category was consistent with its failure to respond coherently to leaks, mistakes, and government relations challenges in 2018. While **Google** scores better than other companies in the Index overall because it discloses more information about more policies in the Freedom of expression and Privacy categories than all other companies (though the high score was a low 63%), it scored lower in the Governance category than all other members of the Global Network Initiative (GNI) who have committed to due diligence and oversight around human rights risks. On the specific indicator examining risk oversight, **Google** was the only U.S.-based company to disclose neither board nor executive-level oversight over risks to either expression or privacy (see Figure 1).

Figure 1 | Governance and Management Oversight

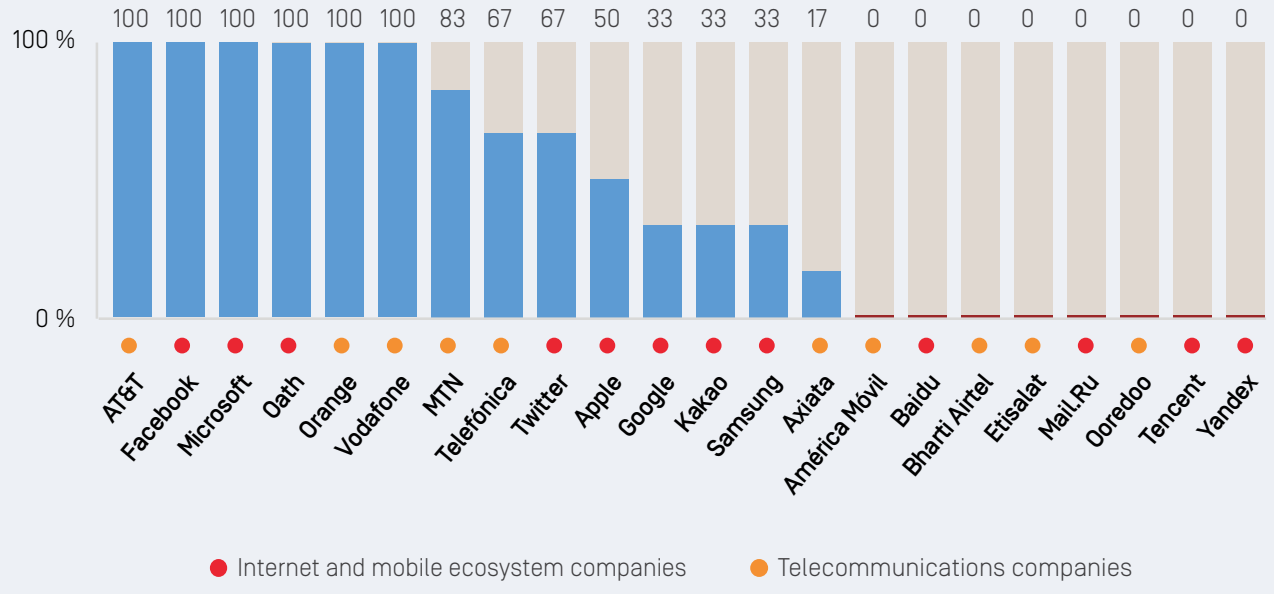
Indicator G2 in the Governance category of the Index is based on the principle that the companies' senior leadership should exercise oversight over how their policies and practices affect freedom of expression and privacy.[1] In order to receive a full score the company must disclose evidence of the following:

1. The board of directors exercises formal oversight over how company practices affect freedom of expression and privacy;

2. An executive-level committee, team, program or officer oversees how company practices affect freedom of expression and privacy;

3. A management level committee, team, program or officer oversees how company practices affect freedom of expression and privacy.

Google disclosed evidence of management level oversight only. Twitter disclosed oversight at the executive level but not the board. Apple disclosed evidence of executive level oversight for privacy but not expression.



The world's most powerful social media platforms disclose no evidence they conduct risk assessments of the impacts of their business models.

Google's nearly two-month silence following initial media leaks about its controversial plans to re-enter the Chinese market is consistent with the company's weak governance and risk management, as identified by RDR's Index findings. Location privacy practices of **Google's** Android mobile operating system are under investigation, and the company continues to face criticism over bias and hate speech in search results and on YouTube. Neither **Google's** CEO, nor the leadership of its parent company **Alphabet**, have presented a clear and consistent vision to shareholders or the public of how the company intends to uphold its commitment as a member of the GNI to respect users' human rights and mitigate the impact of risks across all of its services that potentially affect users' expression and privacy rights worldwide.

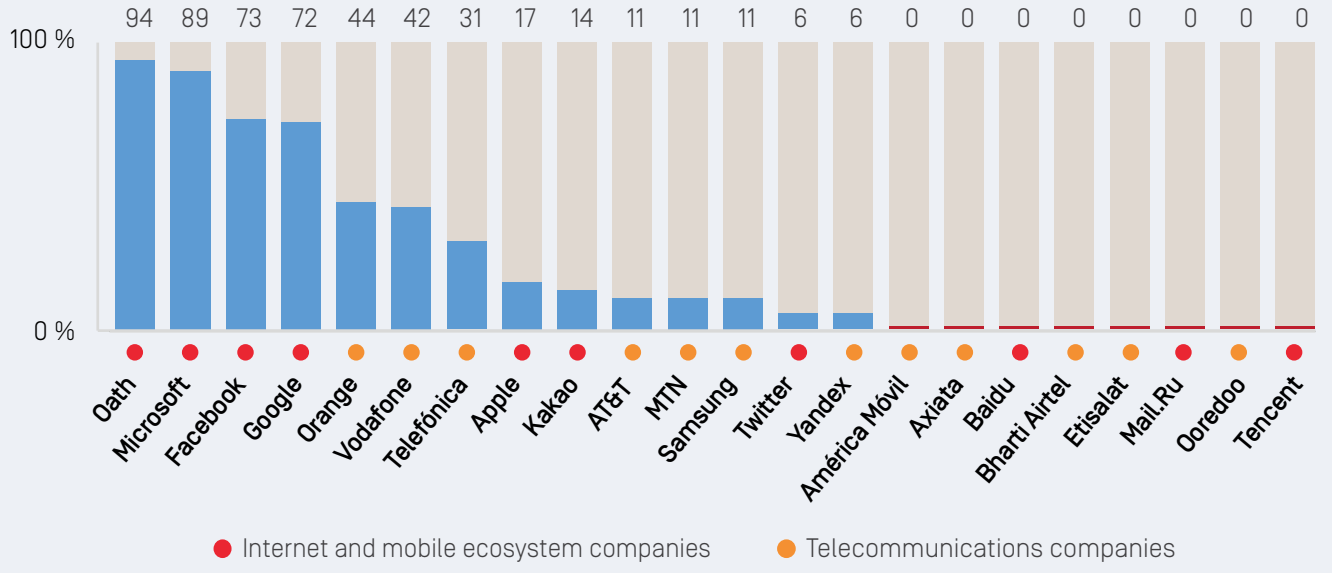
Impact Assessment and Due Diligence

Companies that operate the world's most powerful social media platforms showed no evidence of risk assessment of negative impact on users caused by their business models. GNI-member companies evaluated in the 2018 Index, including **Google** and **Facebook**, all received credit for disclosing evidence that they conduct human rights impact assessments related to the political and regulatory environments in which they operate, including due diligence regarding demands they receive from governments around the world to restrict content or hand over user information.

However, as of the 2018 Index publication, in April 2018, neither **Google** nor **Facebook** disclosed any evidence that they assessed risks caused by their internal processes for moderating and policing content, despite that both companies face growing criticism over its content moderation practices and both companies have consistently identified user-generated content as a target for potential growth. **Twitter** disclosed little evidence of any impact assessment process related to any type of risk. **Apple**, which improved its Index score more than any other company between 2017 and 2018, disclosed that it conducts impact assessments in relation to user privacy, yet offered no evidence that it systematically evaluates risks to users' freedom of expression (see Figure 2).

Figure 2 | Comprehensiveness of Human Rights Impact Assessments

Indicator G4 in the Governance category of the 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 its business on freedom of expression and privacy.[2]



As the sector embraces artificial intelligence and other new technologies, investors should look for evidence that companies are engaging in robust and proactive risk assessment processes, and that boards are taking due diligence seriously.

Index research shows that companies have lacked risk management and due diligence practices related to how online platforms develop and enforce their terms of service—rules that determine what types of content, speech, and behavior are allowed on their services. This risk management gap has serious consequences for users and communities, as well as for companies' long-term business prospects. Even after their global reach and power to shape politics became fully apparent in 2011 with the Arab Spring, companies failed to invest sufficient resources in the development of reliable systems and processes that might have enabled them to tackle hate speech, extremism, and politically incendiary content, while also moderating content in a manner that would also appropriately respect the right of all users to engage in social and political dissent.[3]

The major ICT companies failed to make responsible content governance a priority. This failure occurred despite warnings for the past decade by users, researchers, and public interest groups that platforms' rules and business models were being manipulated to spread disinformation and hate speech, and that clumsily designed enforcement mechanisms were also deleting social media postings by human rights activists and journalists. **Facebook, Twitter** and **Google's** YouTube are only now struggling to retrofit more robust content moderation systems and processes onto platforms and business models that were designed without ample consideration of their impact on public and private discourse around the world.

It is now a regular feature of analyst calls and testimony for companies to point to higher costs resulting from increased resources needed to moderate content and enforce terms of service in an attempt to address problems that have spun out of control. If companies had done more to anticipate and mitigate risks associated with their content governance processes when the problems were more manageable, risk mitigation could have been a source of business model innovation that would create value for users and investors. **Apple** now appears to be benefitting from greater attention to user privacy, underscoring the upside of a business model that does not depend heavily on advertising technology. Yet the company does not disclose evidence of impact assessment on other aspects of its business model that may implicate users' rights, such as the policing of its app store.

Due diligence gaps are a red flag for corporate boards and investors. As the sector embraces artificial intelligence and other new technologies, investors should look for evidence that companies are engaging in robust and proactive risk assessment processes, and that boards are taking due diligence seriously. **Alphabet**, **Google's** parent company, has developed a set of principles around the ethical use of artificial intelligence. This is a laudable start, but the company has yet to disclose evidence that its deployment of AI has been subject to human rights impact assessment. In 2017, **Microsoft** pioneered the industry's first human rights impact assessment for AI, a model which investors might want to see emulated by other companies.[4] For companies that operate complex global platforms with geographically and culturally diverse users, human rights impact assessments can be a powerful tool for identifying and addressing complex and often unanticipated risks before human rights groups and journalists start coming to them with documented cases of harms to individuals and communities.

While AI-related impact assessment was not evaluated in the 2018 Index, we believe that AI will become a new frontier for investors assessing ICT companies' digital rights performance over the next year. As a result, the 2019 Index governance indicators have been broadened to include not only AI and machine learning, but also the role of targeted advertising in the company's business model.[5] Targeted advertising requires that advertisers and marketers (broadly defined to include political operatives and individuals promoting websites) be given access to granular information about users they might want to target. The ability to access personal details about users' personalities, habits and preferences, economic circumstances, and demographics, and target them with content designed specifically to appeal to them, made **Facebook's** social networking platform an attractive conduit for political operatives, governments, and various organizations to

Box 1 | Notable Digital Rights-Related Shareholder Resolutions in 2018

Alphabet/Google—A resolution requiring **regular reporting to investors about Google's efforts to moderate content on its platforms** including YouTube was defeated.[6]

Twitter—A resolution to **report on how the platform enforces its terms of service** to prevent election interference, fake news, hate speech, sexual harassment and violence from being posted to its platform was defeated.[7]

Facebook—Resolutions to create a **board risk oversight committee and require regular reporting on content governance** were defeated.[8] However as a concession the company did change the name of its board audit committee to "audit and risk and oversight committee."[9]

Apple—A **proposal to create a human rights committee** that would report on oversight of the company's human rights risks including freedom of expression failed in 2018. Apple attempted to remove the proposal from the proxy ballot but was overruled by the SEC.[10] A similar proposal, with a stronger focus on freedom of expression, has already been filed for 2019.[11]

As companies' opaque, seemingly arbitrary and unaccountable processes for policing content have come under growing fire over the past three years, they have responded to stakeholder pressure for more transparency.

spread propaganda and disinformation. Yet there has been no evidence that **Facebook** or other companies that rely heavily on targeted advertising including **Google** and **Twitter** have assessed the risks of specific targeted advertising practices and mechanisms to protect users and communities. The regulatory risk related to this issue is highlighted by legalistic disclosures by companies like **Facebook** acknowledging that "user-provided data" related to user age may not be accurate, particularly for young users, and that assumptions about a user's location may also be inaccurate.

Online Speech: Transparency Improves But the Rough Ride Will Continue

RDR's indicators and the Corporate Accountability Index results have proven to be useful in predicting problems that have come to a head in 2018. Following the Index findings and trends can thus yield useful insights for investors. This has certainly proven to be the case with poor corporate transparency around the policing of content. For years the world's most powerful social media platforms have failed to disclose meaningful information about their processes and mechanisms for developing and enforcing terms of service. As a result, regulators and politicians have filled the vacuum with badly designed quick-fix regulations as they themselves come under political pressure to take action against online disinformation, extremism, and bias. While privacy regulation (as discussed in the next section) has for the most part been welcomed by the human rights community, regulatory efforts to hold companies directly liable for users' speech have clashed with valid concerns about the ways in which such laws can be potentially abused for political purposes, even in democracies let alone authoritarian states.

In November 2015 when the first edition of RDR's Corporate Accountability Index was published, no company disclosed any data about content or accounts restricted due to violations of companies' internal rules, community guidelines, or terms of service. As companies' opaque, seemingly arbitrary and unaccountable processes for policing content have come under growing fire over the past three years, companies have responded to stakeholder pressure for more transparency. By the time the third Index was published in April 2018, **Microsoft, Google, Twitter,** and **Facebook** had all begun to release limited information about content and accounts affected by terms of service enforcement. Additional improvements have been made or announced after the 2018 Index data were finalized.[12] There has also been a proliferation of fact-checking and research projects that study and track disinformation and hate speech—many supported by **Google, Facebook,** and **Twitter** in collaboration with journalists, academic researchers, and civil society advocates.

Box 2 | New Online Content-Related Regulation, Proposals, and Government Actions Signal Major Increase in Regulatory Compliance Requirements

Germany—in January 2018, the Network Enforcement Act (NetzDG) went into force, requiring large social networking platforms to remove "illegal content" within 24 hours of receiving a notification, or face fines of up to EUR 50 million. Critics say the law gives private companies too much power to decide what speech should be permitted online and are concerned that companies are over-censoring content to avoid harsh penalties.[13] In early October, Germany's antitrust authority was reported to be assessing whether to take action against **Facebook**.[14]

France—in July 2018, the National Assembly voted to pass legislation that empowers courts to determine whether reports published during an election period should be taken down and allows candidates to sue for the removal of contested reports.[15] The highly contested bills were rejected by the Senate due to concerns about potential abuse of freedom of expression.[16] The Assembly has since passed revisions and the legislation's eventual fate remains unclear.

UK—on September 18, 2018 the media regulator Ofcom outlined a regulatory blueprint for social media that could require greater transparency and impose penalties if inappropriate content is not removed "quickly and effectively." Concrete proposals are expected to be published later this winter.[17] Ofcom is organizing a global conference of regulators early next year to coordinate regulatory responses.[18]

European Union—on September 26, 2018, the European Commission announced that the major internet platforms including **Google**, **Twitter**, and **Facebook** had signed on to a Voluntary Code of Practice in which they committed to empower consumers to report disinformation, support research to monitor and study disinformation, disrupt advertising revenues of accounts and websites that spread disinformation, make political and issue-based advertising more transparent, and proactively work to eliminate fake accounts and curtail online bots that spread disinformation.[19]

USA—in September, President Trump tweeted accusations of anti-conservative bias on search engines and social media, and company executives were questioned about accusations of bias in a congressional hearing.[20] In congressional hearings **Facebook** and **Twitter** have agreed to conduct "civil rights audits" in response to progressive critiques about hate speech and **Facebook** also agreed to conduct a political bias audit.[21] Last year, two democratic senators introduced the Honest Ads Act requiring greater transparency about political advertising.

Brazil—in the months leading to the October 7, 2018 presidential elections, parliament proposed over 15 bills addressing "fake news," many of which sought to criminalize the dissemination of false content. All were opposed by human rights groups concerned that such laws could be abused by government to censor critics.[22]

Malaysia—in August 2018, parliament repealed a "fake news law" passed in April 2018 after it was used by the previous prime minister, Najib Razak, to investigate current Prime Minister Mahatir Mohammed during a contentious election campaign.[23]

Some companies have made efforts to be more transparent about how they police content and about their polices regarding political and issue-based advertising.

These very recent projects and steps taken to improve transparency have come too late to head off new regulatory efforts—many criticized by human rights groups as counterproductive—in a number of countries. Box 2 above lists examples of regulations around the world that target "fake news" and disinformation on social media.

Since the close of RDR's 2018 Index research cycle early in the year, several companies have made improvements in their disclosures about how content is policed in response to government demands or in the process of enforcing terms of service. Companies have also taken a number of important steps in 2018 to improve advertising transparency, especially in relation to political and issue-based ads. Transparency about who is purchasing advertisements on behalf of whom, with what types of messages, is essential for understanding and ultimately addressing online disinformation and propaganda campaigns.

The information that companies started to release in 2018 can help to inform regulatory debates about what types of law will actually be effective in addressing the problems of disinformation and extremism without violating the human rights of many other users. Improved transparency can not only help users who are either victims of hate speech or whose content is deleted or restricted in ways that they believe to be a violation of their

Investors need to develop a frame of reference for evaluating company complaints about the impact of regulatory trends.

rights. Better transparency also helps expert stakeholders including regulators, civil society advocates, and journalists, gain clearer understanding of the volume and nature of content that is restricted or deleted by companies when they enforce their terms of service, as well how the process is carried out. Such understanding is in turn essential to informed public debates about how companies' content policing mechanisms might be improved either through regulation or other multi-stakeholder consultative and decision making mechanisms.

Now that the brave new world of online content and social media is having pervasive impacts on companies' bottom lines, investors will need to develop a frame of reference for evaluating company claims about the impact of regulatory trends. While the nature and impacts of privacy and data protection regulation are fairly well understood, the debate about the impact of regulatory interventions affecting how companies govern users' speech is certain to involve consideration of issues that are unfamiliar to many investors.

For example, human rights experts and advocates have consistently opposed regulation that places strict legal liability on platforms to police content. Their critique is based on concerns about potential abuse of such laws given that definitions of disinformation, hate speech, and extremism are subject to debate even in some of the world's oldest democracies.

Opposition to strict intermediary liability (the legal term) is also due to documented evidence that such laws result in over-censorship: platforms mistakenly take down journalism, advocacy, and political speech that should be protected in accordance with human rights standards. Such over-censorship, also known among human rights activists as "collateral censorship" (echoing military "collateral damage") happens because 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.[32] If companies face steep fines for under-censoring, evidence from around the world where strict liability laws are already in force shows that when in doubt platforms can be expected to over-censor.[33]

Given the human rights risks associated with increasing platforms' liability for users' speech and behavior, experts in communication law and human rights suggest that governments should most constructively focus new legal requirements on the standards and processes for enforcing content policies. For example, companies might be required to

Box 3 | Improved transparency about policies and practices affecting online speech

Below are some examples of new policies by companies aimed at improving transparency of political advertising and content moderation policies and practice since the 2018 Index was published.

Facebook—for the first time in May 2018 published data about its community standards enforcement, along with much greater detail about how its rules are enforced.[24] This followed publication in April of a version of its community standards with much more information about enforcement and appeals than it previously disclosed.[25] The company also launched an archive of political advertising and an ads transparency tool.[26]

Google—in April 2018 published its inaugural YouTube Community Guidelines enforcement quarterly report, containing data about the number of videos removed, what type of content they contained, and what type of process was used to identify and remove them.[27] The company also introduced a new transparency report on political ads.[28]

Twitter—in a transparency report published in April 2018 increased the information and data about accounts or Tweets deleted or restricted after being flagged for terms of service violation by either government officials or non-governmental organizations.[29] It also launched a new Ads Transparency Center.[30]

Apple—announced in May 2018 that starting in the second half of this year it would include data in its bi-annual transparency reports about global government requests to remove applications from its App Store.[31]

establish enforcement processes and mechanisms that are "more transparent, evidence-based, accessible and proportionate" and subject to external review.[34] David Kaye, the UN Special Rapporteur on freedom of expression and opinion, states that companies should engage much more actively with civil society and subject-matter experts to ensure that content policing mechanisms do not fail to achieve their purpose, harm communities, and stifle human rights advocacy. He calls on regulators to focus on "ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums."[35] To guard against abuse of regulations related to online speech, Kaye emphasizes that judicial authorities—not government agencies—should be the arbiters of lawful expression. Governments should release their own data to the public about all content-related requests made of companies. Kaye's recommendations were informed by RDR data and analysis.

Life-and death situations such as the case of Myanmar require rapid responses by companies. However in order to devise appropriate response mechanisms to hate speech that incites ethnic violence, without also over-censoring content from activists and journalists, it is essential that companies conduct human rights impact assessments and establish effective grievance and remedy mechanisms, both of which were discussed in the previous section on governance. Both require special attention to politically sensitive regions, ethnic conflicts, and civil wars in addition to elections.

Privacy and Security: Corporate Irresponsibility Invites More Risk and Regulation

Areas in which disclosure was relatively weak at the start of 2018 foreshadowed how companies have approached their regulatory and compliance posture on privacy and security.

Privacy and data protection risks, and related regulation, are relatively straightforward and familiar to investors than the more complicated controversies related to freedom of expression risks and regulation. RDR's Index data, tracked alongside regulatory trends of the past three years, reveals some interesting patterns that were not otherwise clear enough to investors and boards to prepare them for the events of 2018. Poor disclosure to users about what happens to their data, especially when combined with policies that have limited—or obscured—the amount of control users can have over the collection and sharing of their data, foreshadowed un-examined risks to users' privacy and security that blew up in the headlines this year. Areas where company disclosure was relatively weak at the start of 2018 also foreshadowed how companies have approached their regulatory and compliance posture on data privacy and security.

In the United States until recently, it was normal to hear industry representatives ridicule the EU's General Data Protection Regulation (GDPR) which came into force on May 25, 2018, as an example of excessive governmental meddling in the functioning of some of the world's most innovative companies. That is no longer the case. It is unclear whether corporate leadership of these companies pushed beyond questions of compliance to more fundamental questions of whether they were taking adequate steps to protect individuals from harm—and help people make informed actions to protect themselves from abusive exploitation and theft of their personal information.

By early 2019 the strength and scope of the EU's General Data Protection Regulation (GDPR) enforcement regime will be tested. Notably, the GDPR appears to have spurred policy and disclosure improvements related to privacy and security. All of the companies in the Index with significant numbers of users in the European Union updated and clarified their privacy policies before the GDPR went into force on May 25, 2018. While many policy changes were cosmetic—improving and clarifying language describing existing policies and practices—meaningful improvements were made in a number of cases regarding how users can control the collection of particular types of information and how people can extract data that has been collected about them. **Google** and **Facebook** improved disclosures about how long data is retained.

Box 4 | GDPR-Related Lawsuits, Investigations, and Regulatory Actions

On May 25, 2018, the first day that the GDPR went into force, the privacy advocacy group noyb.eu filed four complaints against **Google** and **Facebook** (along with its WhatsApp and Instagram services) for "forced consent"—requiring that users consent to use their data for advertising purposes in order to use the services at all.[36]

The next day, the French digital rights advocacy organization La Quadrature du Net filed seven complaints against **Facebook**, **Google**, **Apple**, **Amazon** and LinkedIn (**Microsoft**).[37]

In September 2018, EU commissioner in charge of consumer protection, Vera Jourová, warned that **Facebook** must change its "misleading" terms of service before the end of the year.[38]

In September 2018, the privacy-focused browser, Brave, filed a complaint against **Google** in Britain and Ireland alleging the company shares user data with advertisers without their explicit knowledge and seeking an EU-wide investigation on how **Google** and the digital advertising industry are handling people's personal data.[39]

Facebook is under investigation by Irish authorities to determine whether it did enough to protect users' information, per GPDR standards, following the company's announcement in September 2018 of a data breach affecting 50 million users.[40]

However, these steps may end up falling short of what companies need to do in order to genuinely protect users from harm. It will soon become clear how aggressively the GDPR will be interpreted and enforced. Privacy advocates and regulators have already begun to probe and challenge these companies' GDPR compliance. Box 4 (above) offers a list of lawsuits, regulatory actions, and investigations currently under way.

The 2018 Index results on indicators related to the handling of user information foreshadowed some of the challenges that companies now face.

RDR does not evaluate GDPR compliance. However, the 2018 Index results on indicators evaluating transparency and responsible policy around the handling of user information did foreshadow some of the challenges that companies now face. Specifically, the 2018 Index data showed that **Google** and **Apple** disclosed less about what user information they share with whom than all other internet and mobile companies evaluated in the Index except for Mail.ru of Russia and Baidu of China.[41] **Facebook** offered fewer options for users to control what information the company collects, retains, and uses than any other internet or mobile platform in the 2018 Index (see Figure 3 on next page).[42]

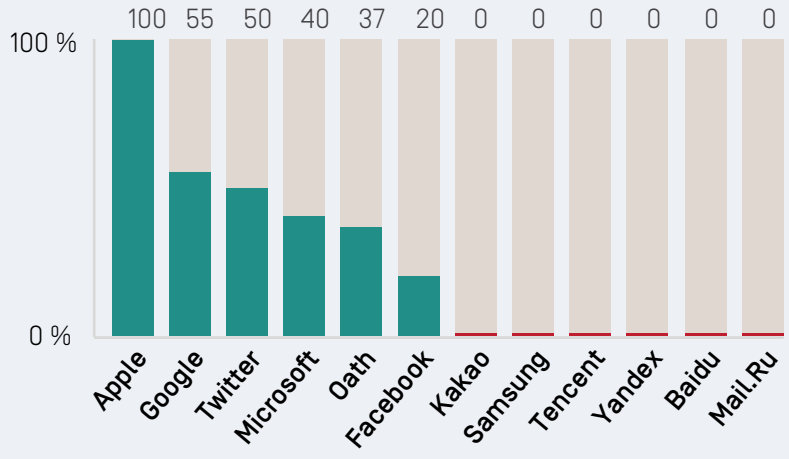
In the 2018 Index, **Apple** stood out for being the only internet or mobile company that clearly stated that it does not track users across third party websites or applications. Five other companies disclosed with varying amounts of specificity that they do track users across the internet, and six did not offer any disclosure about their tracking practices. **Apple's** commitment to refrain from tracking is easier because its business model does not depend on the collection of data about users' activities outside its own platforms.

Going forward, investors will be wise to monitor which companies are moving fast to develop business models that are compatible with responsible stewardship of personal data, even if that means leaving some advertising revenue on the table in the short term. The risk of short-term gain over long-term responsibility is that companies will become overly reliant on business models that cannot survive regulatory pushback as technologies evolve from being novel and exciting to more widespread and powerful.

The regulatory outlook in the United States changed dramatically in the past year and will continue to evolve rapidly. At the time of the publication of our previous investor research note in September 2017, there appeared to be little appetite at the national level for privacy regulation. However the Cambridge Analytica scandal in early 2018, followed by California's passage of a new privacy law over the summer, has led to a corporate lobby for national privacy legislation that would set a lower bar than California's but supersede it.[43] Privacy advocates are calling for a national law that states could potentially build upon with more stringent requirements.[44] Meanwhile a number of states have passed

Figure 3 | Whether Companies Commit Not to Track Users Across the Internet

The chart below is based on data collected through January 2018. In the 2018 Index, Apple stood out for being the only company to clearly state it does not track users across third-party websites or applications. (See page 10 for full discussion).



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

2019 is promising to be a very active year for privacy regulation and enforcement—on both sides of the Atlantic but also beyond.

specific privacy-related provisions.[45] States are also growing more aggressive with investigations in relation to alleged privacy violations: The Arizona attorney general is investigating **Google** for data collection practices of its Android operating system.[46]

2019 is promising to be a very active year for privacy regulation and enforcement—not only on both sides of the Atlantic but also beyond. In India, a new data protection bill is expected to be introduced in parliament before the end of the year, following last year's landmark Supreme Court judgment declaring privacy to be a fundamental human right.[47] The details are already subject to intense domestic and international lobbying. Across the world, regulation that protects consumers from deceptive, discriminatory, and exploitative uses of their data, or data collection and sharing that enables citizens to be targeted by disinformation campaigns, should be welcomed for the same reasons many investors and companies have come to welcome regulation that addresses climate change or promotes environmental sustainability.

2019 and beyond

2018 was the harbinger of more to come. From an investor perspective, the Silicon Valley internet giants can no longer be considered low risk. RDR's indicators and Index data, plus complementary research produced by our growing network of partners, can help investors prepare for what is coming next.

The 2019 Index will be published in May, covering 24 companies. Most of the indicators have remained the same, except for the Governance section: the indicator on risk assessment contains new elements covering targeted advertising, algorithms and machine learning, and the indicator focused on grievance and remedy was revised to align more closely to the UN Guiding Principles. Notably, the 2019 Index will take a closer look at cloud computing services.

While RDR is in no way an evaluation of GDPR compliance, the degree of change in privacy scores between 2018 and 2019 will nonetheless offer some helpful perspective on the extent to which the GDPR spurred meaningful changes to company policy and disclosure, versus cosmetic and semantic changes.

Beyond 2019, future indexes will include more company types, and new indicators covering emerging issues. Our research team is now carrying out preliminary research toward determining how the existing indicators will need to be adapted so that Amazon and Alibaba can be added to future indexes. Before then, we hope to publish some pilot research on these companies.

We are working to develop new indicators that will enable closer scrutiny of company disclosures related to how targeted advertising and the use of algorithms and machine learning affect users' privacy and expression rights. Along the way, we also hope to publish some preliminary research on these topics that should be helpful to investors looking to engage with companies on these issues.

We look forward to hearing from investors who use our indicators and data. For more information please contact Rebecca MacKinnon at: mackinnon@rankingdigitalrights.org.

Box 5 | Other Research Organizations Have Adapted RDR's Open Methodology

- RDR's methodology and indicators are openly available and licensed under the Creative Commons Attribution 4.0 International License.
- Researchers around the world have applied the Index methodology to evaluate companies in local and regional markets. A list of projects that have published results thus far can be found at: https://rankingdigitalrights.org/adaptations/.
- RDR partnered with Consumer Reports and other organizations specializing in technical testing and research to produce a set of criteria for evaluating the privacy and security of applications and devices that make up the "internet of things." The resulting Digital Standard framework can be found at: https://www.thedigitalstandard.org.
- Consumer Reports has used the Digital Standard in evaluations of smart TV's and payment apps.[48]

Key questions to ask companies

The following ten questions can help investors evaluate whether companies are making adequate efforts to respect users' rights, thereby mitigating individual harms and broader business risks. These questions are also a useful starting point for investor engagement with companies, particularly when combined with the key findings and recommendations from the individual company report cards published with the Index.

1. Risk assessment: Has the company management identified digital rights risks that are material to its business and does the company carry out impact assessments on the full range of these risks? Does it disclose any information about whether and how the results of assessments are used?

2. Oversight: Does the board exercise direct oversight over risks related to user security, privacy, and freedom of expression? Does board membership include people with expertise and experience on issues related to digital rights?

3. Stakeholder engagement and accountability: Is the company a member of the Global Network Initiative (GNI) and if not, why not?

4. Transparency about data collection and use: Does the company disclose clear information about its policies and practices regarding collection, use, sharing, and retention of information that could be used to identify, profile or track its users?

5. Transparency about handling of government demands and other third party requests affecting users' expression and privacy rights: Does the company disclose policies for how it handles all types of third-party requests (by authorities or any other parties) to share user data, restrict content, restrict access, or shut down service (including network shutdowns by telecommunications companies)?

6. Transparency reporting: Does the company publish data about the volume and nature of the requests it receives, and responds to, for: sharing user data, restricting content or accounts, shutting down networks? Does it also publish data about the volume and nature of content and accounts restricted in the course of enforcing its own terms of service?

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

8. Encryption: Does the company commit to implementing the highest encryption standards available for the particular product or service? If not, why not?

9. Mobile security: Do companies that operate mobile ecosystems disclose clear policies about privacy and security requirements for third-party apps?

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

Notes

1 For full results and data see "G2: Governance and management oversight," Ranking Digital Rights 2018 Corporate Accountability Index, April 25, 2018, https://rankingdigitalrights.org/index2018/indicators/g2/.

2 "G4: Impact assessment," Ranking Digital Rights 2018 Corporate Accountability Index, April 25, 2018, https://rankingdigitalrights.org/index2018/indicators/g4/.

3 See "3.4 Spotlight: Human rights impact assessments," Ranking Digital Rights 2018 Corporate Accountability Index, April 25, 2018, https://rankingdigitalrights.org/index2018/report/inadequate-disclosure/#section-34.

4 "Microsoft Salient Human Rights Issues: Report - FY17," (Microsoft, 2018), http://download.microsoft.com/download/6/9/2/692766EB-D542-49A2-AF27-CC8F9E6D3D54/Microsoft_Salient_Human_Rights_Issues_Report-FY17.pdf.

5 "2019 Indicators," Ranking Digital Rights, September 2018, https://rankingdigitalrights.org/2019-indicators/.

6 Meaghan Kilroy, "Shareholders reject proposals for Alphabet to move to one vote per share, report on content enforcement," Pensions & Investments Online, June 8, 2018, http://www.pionline.com/article/20180608/ONLINE/180609882/shareholders-reject-proposals-for-alphabet-to-move-to-one-vote-per-share-report-on-content-enforcement.

7 Meaghan Kilroy, "Proposal to report on efforts to prevent fake news supported by 36% of Twitter shareholders," Pensions & Investments Online, June 4, 2018, http://www.pionline.com/article/20180604/ONLINE/180609956/proposal-to-report-on-efforts-to-prevent-fake-news-supported-by-36-of-twitter-shareholders.

8 Meaghan Kilroy, "Facebook shareholders defeat voting structure, risk oversight proposals," Pensions & Investments Online, June 6, 2018, http://www.pionline.com/article/20180606/ONLINE/180609914/facebook-shareholders-defeat-voting-structure-risk-oversight-proposals.

9 Sara Fischer, "Facebook changes audit committee charter after privacy issues," Axios, June 15, 2018, https://www.axios.com/facebooks-board-expands-role-of-a-1529004696-6d97c141-2709-4eb5-8fe4-b893b782f7cc.html.

10 "USA: Apple pushes back on shareholder proposals related to human rights and climate issues," Business & Human Rights Resource Center (BHRRC), January 8, 2018, https://www.business-humanrights.org/en/apple-pushes-back-on-shareholder-proposals-related-to-human-rights-climate-issues.

11 Peter Flaherty, "Apple Shareholder Files Proposal on Free Speech," National Legal and Policy Center, August 28, 2018, http://nlpc.org/2018/08/28/apple-shareholder-files-proposal-on-free-speech/.

12 "Policing speech," Ranking Digital Rights 2018 Corporate Accountability Index, April 25, 2018, https://rankingdigitalrights.org/index2018/report/policing-speech/.

13 Emma Thomasson, "Germany looks to revise social media law as Europe watches," Reuters, March 8, 2018, https://www.reuters.com/article/us-germany-hatespeech/germany-looks-to-revise-social-media-law-as-europe-watches-idUSKCN1GK1BN .

14 Ali Breland, "German antitrust watchdog 'optimistic' Facebook enforcement action will come later this year," The Hill, October 1, 2018, https://thehill.com/policy/technology/409233-german-antitrust-watchdog-very-optimistic-on-facebook-enforcement-action .

15 Zachary Young, "French Parliament passes law against 'fake news,' Politico, July 4, 2018, https://www.politico.eu/article/french-parliament-passes-law-against-fake-news/.

16 French Senate press release, October 11 2018, https://www.senat.fr/espace_presse/actualites/201806/lutte_contre_les_fausses_informations.html.

17 Aliya Ram and Nic Fildes, "Ofcom outlines case for regulating social media networks, Financial Times, September 18, 2018, https://www.ft.com/content/a16935a4-bb39-11e8-94b2-17176fbf93f5.

18 Lucy Handley, "Regulators around the world are shaping up for a social media crackdown," CNBC, September 20, 2018, https://www.cnbc.com/2018/09/20/social-media-regulation-ofcom-organizing-international-meeting.html.

19 "Code of Practice on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

20 Cecilia Kang and Sheera Frenkel, "Republicans Accuse Twitter of Bias Against Conservatives," The New York Times, September 5, 2018, https://www.nytimes.com/2018/09/05/technology/lawmakers-facebook-twitter-foreign-influence-hearing.html.

21 Josh Constine, "Twitter agrees to abuse-transparency reports, civil rights audit," TechCrunch, September 5, 2018, https://techcrunch.com/2018/09/05/government-vs-twitter/.

22 Ernesto Londoño, "Brazil Looks to Crack Down on Fake News Ahead of Bitter Election," The New York Times, February 17, 2018, https://www.nytimes.com/2018/02/17/world/americas/brazil-election-fake-news.html and Veridiana Alimonti, "Fake News and Elections in Brazil: Several Initiatives, No Easy Answer," Electronic Frontier Foundation, October 2, 2018, https://www.eff.org/deeplinks/2018/09/fake-news-and-elections-brazil-several-initiatives-no-easy-answer.

23 Hannah Ellis-Petersen, "Malaysia scraps 'fake news' law used to stifle free speech," The Guardian, August 17, 2018, https://www.theguardian.com/world/2018/aug/17/malaysia-scraps-fake-news-law-used-to-stifle-free-speech.

24 Guy Rosen, "Facebook Publishes Enforcement Numbers for the First Time," Facebook Newsroom, May 15, 2018, https://newsroom.fb.com/news/2018/05/enforcement-numbers/.

25 Monika Bickert, "Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process," Facebook Newsroom, April 24, 2018, https://newsroom.fb.com/news/2018/04/comprehensive-community-standards/.

26 Anthony Ha, "Facebook will allow you to see all the active ads from any Page," TechCrunch, June 28, 2018, https://techcrunch.com/2018/06/28/facebook-ad-transparency/.

27 The YouTube team, "More information, faster removals, more people – an update on what we're doing to enforce YouTube's Community Guidelines," Google Blog, April 23, 2018, https://youtube.googleblog.com/2018/04/more-information-faster-removals-more.html.

28 Michee Smith, "Introducing a new transparency report for political ads," Google Blog, August 15, 2018, https://www.blog.google/technology/ads/introducing-new-transparency-report-political-ads/.

29 Twitter Public Policy, "Expanding and building #TwitterTransparency," Twitter Blog, April 5, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/twitter-transparency-report-12.html.

30 Bruce Falck, "Providing more transparency around advertising on Twitter," Twitter Blog, June 28, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Providing-More-Transparency-Around-Advertising-on-Twitter.html.

31 Ashley Carman, "Apple will start reporting government requests to remove apps from the App Store," The Verge, May 25, 2018, https://www.theverge.com/2018/5/25/17396512/apple-transparency-report-app-takedown-requests.

32 See for example: Thant Sin, "Facebook Bans Racist Word 'Kalar' In Myanmar, Triggers Collateral Censorship," Global Voices Advox, June 2, 2017, https://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, https://medium.com/@thedididelgado/mark-zuckerberg-hates-black-people-ae65426e3d2a .

33 "Fostering freedom online: the role of internet intermediaries," (UNESCO Publications and Communications Materials, 2015), http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/fostering-freedom-online-the-role-of-internet-intermediaries/.

34 Mark Bunting, "Regulating online platforms for misinformation and disinformation," Media Policy Project at London School of Economics, September 27, 2018, http://blogs.lse.ac.uk/mediapolicyproject/2018/09/27/regulating-online-platforms-for-misinformation-and-disinformation/.

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

36 Lucy Fielder and Douglas Busvine, "Austrian data privacy activist takes aim at 'forced consent,'" Reuters, May 25, 2018, https://www.reuters.com/article/us-europe-privacy-lawyer/austrian-data-privacy-activist-takes-aim-at-forced-consent-idUSKCN1IQ0ZI.

37 "Filing of collective complaints against GAFAM!" La Quadrature du Net, May 28, 2018, https://www.laquadrature.net/en/node/10532.

38 Jennifer Rankin, "EU warns Facebook it faces sanctions over 'misleading' T&Cs," The Guardian, September 20, 2018, https://www.theguardian.com/technology/2018/sep/20/eu-warns-facebook-faces-sanctions-misleading-terms-conditions-data.

39 Douglas Busvine, "Mozilla co-founder's Brave files adtech complaint against Google," Reuters, September 12, 2018, https://www.reuters.com/article/us-europe-privacy-complaint/mozilla-co-founders-brave-files-adtech-complaint-against-google-idUSKCN1LS2JL.

40 "The EU's new privacy law is starting to bite Facebook," The Economist, October 6, 2018, https://www.economist.com/business/2018/10/06/the-eus-new-privacy-law-is-starting-to-bite-facebook.

41 "P4: Sharing of user information," Ranking Digital Rights 2018 Corporate Accountability Index, April 25, 2018, https://rankingdigitalrights.org/index2018/indicators/p4/.

42 "P7: Users' control over their own user information," Ranking Digital Rights 2018 Corporate Accountability Index, April 25, 2018, https://rankingdigitalrights.org/index2018/indicators/p7/.

43 Cecilia Kang, "Tech Industry Pursues a Federal Privacy Law, on Its Own Terms," The New York Times, August 26, 2018, https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html.

44 Alfred Ng, "Privacy advocates tell senators what they want in a data protection law," CNet, October 10, 2018.

45 See a list at Jeewon Kim Serrato, Chris Cwalina, Anna Rudawski, Tristan Coughlin, and Katey Fardelmann, "US states pass data protection laws on the heels of the GDPR," Data Protection Report, July 9, 2018, https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

46 Greg Sterling, "Report: Arizona attorney general investigating Google location tracking," Marketing Land, September 7, 2018, https://marketingland.com/report-arizona-attorney-general-investigating-google-location-tracking-247965.

47 Vasant Dhar, "Who controls your data? India may pass a law ensuring that you do." The Washington Post, September 25, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/09/25/who-controls-your-data-india-may-pass-a-law-ensuring-that-you-do/ and "IT Ministry gets over 400 responses on draft personal data protection bill," The Economic Times, October 11, 2018, https://economictimes.indiatimes.com/tech/internet/it-ministry-gets-over-400-responses-on-draft-personal-data-protection-bill/articleshow/66164268.cms.

48 See Consumer Reports Press Release, 6 August 2018 https://www.consumerreports.org/media-room/press-releases/2018/08/_consumer_reports_releases_its_first_ever_peer_to_peer_payment_services_ratings/ and Consumer Reports Press Release, 7 February 2018 https://www.consumerreports.org/media-room/press-releases/2018/02/consumer-reports-finds-smart-tvs-vulnerable-to-hacking/.

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, please visit https://rankingdigitalrights.org.

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

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

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.