Poor Digital Rights Performance—Who Pays the Price?

SEPTEMBER 21, 2017

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

Rebecca MacKinnon
Director, Ranking Digital Rights

Users are already paying a price, with implications for investors.

This research note introduces global investors to the evaluation framework, analysis and data produced by Ranking Digital Rights, which ranks the world's most important internet, mobile, and telecommunications companies on disclosed policies affecting users' privacy and freedom of expression.

The goal is to build investor awareness of potential material risks related to digital rights in order to inform investment research and decisions, and to support investor engagement with companies on these issues.

- **Digital rights provide a framework for evaluating risks associated with the management and use of content and personal data by companies that provide highly valued digital services upon which people increasingly depend.** In this growing ecosystem of paid and free services, customers often grant companies the right to access information about their lives and businesses, as well as power to restrict users' ability to publish, transmit, or access content. The result is that companies are granted tremendous power over nearly every aspect of users' lives affected by digital communications—from the intimately personal to the financial and political.

- **The financial implications of digital rights issues are growing rapidly, reshaping how investors should think about risk profiles of companies that provide services affecting consumer privacy, data security, and management of content affecting users' freedom of expression.** These new, often unexamined issues can be monitored by analyzing core company policies and disclosures about practices related to security and handling of user data; company responses to governments seeking to block online information or shut down communications; and companies' use of private mechanisms to manage content and data.

- **This brief highlights the value of the RDR Corporate Accountability Index as a leading indicator for what are potentially the most material digital rights business and investment risks.** Evaluating 22 of the world's most powerful internet, mobile, and telecommunications companies against a robust methodology, the Index highlights inadequate disclosure and commitment. The 2017 Index showed that Google and Microsoft led their internet peers in making key disclosures, while leaving substantial room for improvement. AT&T and Vodafone were at the top of the telecom rankings, albeit with scores of under 50 percent. Performance is diverse with companies like South Korea's Kakao and India's Bharti Airtel outperforming on select metrics. Yet important mobile communications leaders such as Apple and Samsung are notable laggards, particularly on their governance of these risks.

- **The highest risk issues for investors identified by the Corporate Accountability Index were:**

  - Security breaches and the lack of clarity about measures to secure user data;
  - Erratic disclosure of privacy protections and inadequate policies for responsible handling of user data; and
  - Failure to address growing demands by governments to shut down networks in the developing world.

The 2017 Index results also shed new light on regulatory uncertainty around privacy and net neutrality in the United States as well as emerging competition among leading internet, smartphone and network operators on improved disclosure and consumer security protections. Alert investors will find valuable company engagement opportunities as a result.

About the Ranking Digital Rights Corporate Accountability Index

Published in March 2017, the Ranking Digital Rights 2017 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/index2017. The next Index will be released in April 2018.

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,[1] 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,[2] 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.

For the full set of 2017 indicators see: https://rankingdigitalrights.org/2017-indicators/

Company results by indicator: https://rankingdigitalrights.org/index2017/indicators/

To download the full Index dataset and printable PDFs of the Index report and company report cards please visit: https://rankingdigitalrights.org/index2017/download/

For most investors, digital rights issues have been hiding in plain sight for more than a decade.

Impact and Market Relevance of Digital Rights

For most investors, digital rights issues have been hiding in plain sight for more than a decade. The issues are complex—reflecting global markets and regulation as well as the ad hoc emergence of norms around how online services manage content and user data—making it hard for many investors to recognize the potential significance of specific abuses or to track evolving performance standards. Moreover, the business model for internet services, including telecoms, involves many unpriced externalities, as demonstrated by a broad array of risks that have been effectively outsourced to a fragmented user base with little bargaining power. A consistent pattern of service and privacy violations has emerged, as companies face challenges of policing user–generated content, in addition to legal and regulatory actions.

For investors, any assessment of materiality naturally turns on both the financial and strategic impact of digital rights events and their frequency. One-off, high impact events due to unusual circumstances are damaging but those that persist and reflect systemic market or regulatory risks have very different financial implications for seasoned investors with fiduciary obligations. A review of incidents related to digital rights issues tracked by the investment research firm, Sustainalytics, shows a sharp increase in incidents since 2010 related to the companies covered in the Index. For example, in 2009, the only incident cited related to MTN's operations in Iran, but in 2016 a diverse range of 161 incidents was recorded, reflecting a growing range of content takedowns, hacking, and data privacy abuses. This trend is on course to accelerate in 2017, with 87 incidents recorded in 1Q 2017 alone, suggesting an annualized figure of 348, marking a year-over-year increase of 116%.

The table below highlights a selection of relevant digital rights-related incidents from data provided by Sustainalytics through the end of 2016. Persistent digital rights problems include data breaches like those suffered by Yahoo users, Facebook's challenges in handling extremist content and fake news, a constellation of privacy violations related to data sharing across platforms, and the role of telecom and internet companies in providing private user data to governments.

Figure 1 | Issue Snapshot—Diverse and Persistent Problems

Date	Selected company incidents related to digital rights	Companies
2009	Post-election network shutdown; surveillance-related privacy violations	MTN Irancell
2011	Network shutdown and service issues in Egypt during Arab Spring	Vodafone
2011	Exposure & critique by privacy advocates of collection/handling of geo-location data on devices	Apple
2012	Russian hacker steals millions of passwords	Microsoft (Linkedin)
2012	Provided user data to political campaigns for targeted ads	Microsoft, Yahoo
2012	Pays US$22 mn to settle claims related to misuse of Safari browser privacy settings	Google (Alphabet Inc.)
2013	Accusations that the Bing search engine censored searches for Chinese users	Microsoft
2013	Multiple reports concerning sharing of user data with the NSA PRISM program	Apple, Facebook, Microsoft (Linkedin), Yahoo
2013	Suit filed concerning the transfer of EU user data to non-EU servers without a security protocol	Apple, Facebook, Microsoft
2013	Claims that Vodafone shared user data with the UK GCHQ Tempora program	Vodafone
2013	Settles suit for US$20 mn concerning use of users names and images for advertisements	Facebook
2014	Companies confirm regular sharing of user data in response to NSA requests	Alphabet, Apple, Facebook, Microsoft, Yahoo
2014	Confirms that celebrity photos were hacked from iCloud. Increases user security protocols.	Apple
2014	Accused of ignoring complaints about account security and the creation of false accounts	Twitter
2015	Complaints about Windows 10 and poor privacy management	Microsoft
2016	Disclosed that Yahoo! Agreed to an NSA request to scan and share incoming email	Yahoo
2016	Hemisphere data is sold to local US police departments, only an administrative supoena is required	AT&T
2016	Google notifies Microsoft of a security flaw in Windows 10 being exploited by state backed hackers	Microsoft
2016	Studies claim that WeChat censors information for China-registered users even outside of China	Tencent
2016	EU regulators threaten companies with new regulation over terrorist content and hate speech	Alphabet, Facebook, Microsoft, Twitter
2016	Yahoo! discloses two data breaches affecting 1.5 mn users	Yahoo

Source: Sustainalytics

A few companies have begun to flag digital rights issues as material to their business in public statements and disclosures. In 2013, Microsoft General Counsel Brad Smith famously called the NSA's efforts to circumvent the company's security protections for user communications an "advanced persistent threat" to Microsoft's global business.[3] In its 2017 sustainability report, Vodafone listed digital rights, including privacy, data protection and security as being the first of 10 priorities in the company's 'materiality matrix'.[4]

Another powerful indication of the scope and materiality of digital rights issues was the "Risk Factor" section of Snap Inc.'s recent IPO filing. The popular messaging company is too new to be assessed in the Index. However as a high-profile newly listed app company with an IPO valuation of US$3.4 billion in March 2017, Snap's required IPO disclosures offer a timely legal interpretation of the many ways that the company's business model could be damaged by common digital rights challenges that may result in liability risks for the company and share price performance problems for its investors. In addition to citing potential risks related to Snap's products, it also highlights Snap's exposure to the risk profile of mobile ecosystem operators and the fast-changing regulatory landscape.

Figure 2 | Digital Rights Issues that May Affect Snap

Snap Inc's Risk Factor disclosures included prominent disclosure of the following issues:

Our ecosystem of users, advertisers, and partners depends on the engagement of our user base. We anticipate that the growth rate of our user base will decline over time. If we fail to retain current users or add new users, or if our users engage less with Snapchat, our business would be seriously harmed.

There are many factors that could negatively affect user retention, growth, and engagement, including if:

- our products fail to operate effectively on the iOS and Android mobile operating systems;
- we are unable to combat spam or other hostile or inappropriate usage on our products;
- there are concerns about the privacy implications, safety, or security of our products;
- there are changes in our products that are mandated by legislation, regulatory authorities, or litigation, including settlements or consent decrees that adversely affect the user experience;
- we, our partners, or other companies in our industry are the subject of adverse media reports or other negative publicity;
- we do not maintain our brand image or our reputation is damaged

Any decrease to user retention, growth, or engagement could render our products less attractive to users, advertisers, or partners, and would seriously harm our business.

Source: Snap S-1, filed 16 February 2017
Archived at https://investor.snap.com/financial-information/sec-filings

Just as the nature and material relevance of digital rights related incidents has come into focus, so have reference points for investors who must assess the potential financial impact of digital rights issues on broadly held index-sensitive companies. Yahoo's announcement that the value of their planned acquisition by Verizon would be reduced by a minimum of US$350 million due to customer hacking damages should be viewed as a realistic indication of the value and brand destruction that can result from bad management of data security risks. Yahoo's poor management of its security risks and breaches has had a material impact on its users and investors alike. Indeed, it is reasonable to assume that some of the disclosures would never have been made if Yahoo had not been subject to due diligence by potential acquirers. This predicament goes to the heart of the valuation issue. Verizon as a potential buyer, with the benefit of full but confidential disclosure by Yahoo, was able to extract an economic advantage from Yahoo which penalized Yahoo's equity investors. Not only did Yahoo give up US$350 million in transaction value, but it also agreed to share costs which might result from any subsequent legal liabilities related to the security breaches.

It is now possible to identify portfolio risks and engagement priorities that could be appropriate to active, long-term investors exposed to high value equities with significant digital rights risks.

Government-directed network shutdowns have also become a powerful indicator of the costs of restricting access to the internet as businesses and critical public services grind to a halt. Estimates from the Brookings Institution indicate that network shutdowns resulted in broad economic losses across multiple countries of US$2.4 billion based on an examination of known cases from July 2015 through June 2016.[5]

Over the past year there has been a spate of privacy controversies related to high-value smartphone apps. Uber was accused in early 2017 of inappropriately retaining user data and restricting service. In mid 2017, Apple complied with Chinese government demands to restrict Chinese users' access to important security tools such as virtual private network (VPN) apps. These events have highlighted the complicated gatekeeping role for users' digital rights by the dominant mobile operating system companies, Google (Alphabet, Inc.), Apple, and Samsung. Via the devices and operating systems produced by these companies, users access the internet primarily through software applications or "apps" downloaded onto the device via app stores. Access to the app stores is often a matter of market viability for mobile-supported app companies, but accountability norms related to privacy, security, and freedom of expression are weak. Disclosure by companies that control app stores about how they decide what apps are available in which markets and under what conditions is erratic. This information gap makes it hard for investors to assess claims about the app companies' ability to access markets. Weak disclosure by app companies about the collection, handling, and sharing of user information points to unsustainable monetization strategies fraught with regulatory, security, and reputational risks.

Ranking Digital Rights 2017 Index Key Findings for Investors

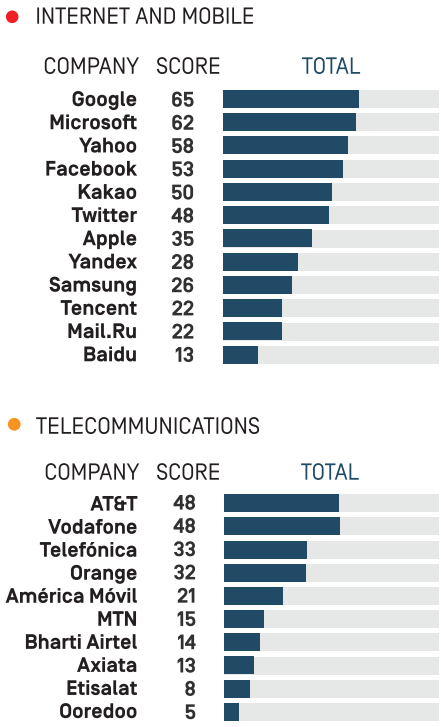
The results of the 2017 Index, discussed in more detail below, highlight a range of complex and strategic issues affecting listed internet and telecommunications companies. With a collective market capitalization in excess of US$3.0 trillion, the 22 internet and telecom companies in the Index have a significant impact on the performance of global portfolios and key indices such as the S&P 500. Using the Index findings and related analysis, it is now possible to identify portfolio risks and engagement priorities that could be appropriate to active, long-term investors exposed to high value equities with significant digital rights risks.

Across the board, there was inadequate disclosure about the risks and constraints people face when using digitally networked products, services, and platforms. The Index results revealed that even if one is persistent enough to pore over terms of service and parse through privacy policies it is impossible to formulate a clear picture of the ranked companies' policies affecting users' digital rights. It is equally difficult for investors to gain a clear picture of how these companies manage key risks affecting users' confidence in their products and services, even as a search of news databases points to rising levels of risk. As a result, the risks are in effect passed on by companies to their customers and users in ways that can impair value for investors, especially if legal and regulatory risks are badly managed as we have seen with Yahoo.

While company disclosures related to user privacy and security are generally poor, most companies offer even less disclosure to users about how the services, platforms and devices they depend upon manage or restrict information flows, access to content, and even access to the internet itself. This issue divides the interests of many content providers in the net neutrality debate[6] and can shape the growth trajectory of companies like Snap that rely on critical infrastructure provided by others.

Companies failed to communicate how regulatory compliance affects end users, whether positively or negatively. Even in jurisdictions where privacy regulations are strong, companies failed to disclose how such compliance helps to protect user privacy and security. In cases where regulation (e.g., government censorship or surveillance

Figure 3 | Overall 2017 Rankings of Internet and Telecommunications Companies



requirements) or commercial considerations (e.g., prioritization of access to certain types of content or services while blocking or making it more difficult access to others) may have negative implications for users' digital rights, companies generally failed to provide adequate disclosure about when, how, and why user data was shared or users' ability to access, publish, or transmit content was restricted.

The Index results expose the extent to which most of the world's internet users lack the information they need to make informed choices about what platforms and services to use or how to use them safely.

Similar to the results from RDR's inaugural 2015 Index, the average score for all 22 companies evaluated was just 33 out of 100—and no company in the 2017 Index scored more than 65 overall. Although there has been improvement since 2015, even the best performing companies had significant gaps in their disclosure, raising questions about their ability to meet stakeholder expectations as public awareness and media attention around these issues continues to grow. The Index results expose the extent to which most of the world's internet users lack the information they need to make informed choices about what platforms and services to use or how to use them safely. Investors must be increasingly alert to the possibility of unmanaged risks and unstable business models.

The overall rankings also highlight a key theme of the Index—although there are clear leaders, performance is differentiated. While many differences are caused by wide variations in regulatory environments of the companies' home countries, other differences (particularly between the various U.S.-based internet and mobile companies, and between the two Korean companies) raise important questions about why different companies headquartered in the same jurisdictions approach well recognized issues in such different ways—and whether they have adequate governance, management, and policy frameworks in place to manage the associated risks.

While Google ranked first in both the 2015 and 2017 Indexes, reflecting greater over-all volume disclosure of more policies related to digital rights than other companies, Microsoft is closing in. This shift was due in part to Microsoft's improved disclosure since the 2015 Index of policies affecting freedom of expression in particular and other human rights concerns in general. Meanwhile, Google's lead in the Index narrowed in 2017 due mainly to the addition of Google's Android mobile operating ecosystem to the Index coverage, for which the company disclosed less information than for the other Google services evaluated. Meanwhile, AT&T and Vodafone tied for first place among telecommunications companies—albeit with only 48 out of 100 possible points, highlighting serious gaps in both companies' disclosed policies. For full comparative data on how each of the 22 companies scored on each of the 35 index indicators please visit rankingdigitalrights.org/index2017.

See **Figure 4** for a selection of findings likely to be of particular interest to investors.

Figure 4 | Notable Company Disclosures—Largely a Mixed Bag

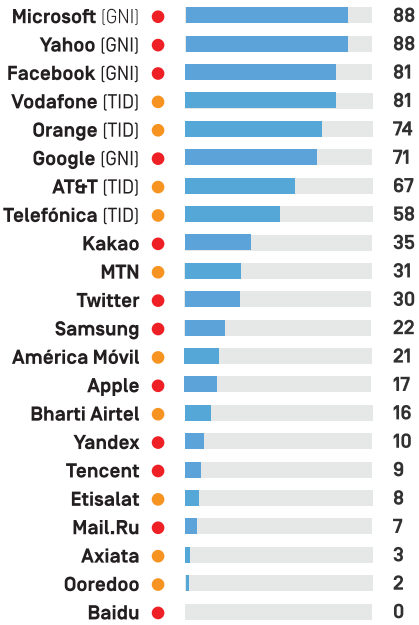
Selected Indicator Findings from the RDR 2017 Corporate Accountability Index
With the debate about net neutrality coming into focus, **Vodafone** stands out as the only telecommunications company evaluated to make an explicit commitment not to block or prioritize content in its home market.
Only three companies—**Telefonica**, **AT&T**, and **Vodafone**—disclosed any information about the process for responding to data breaches. **AT&T** stood out for its disclosure on how it handles government requests for user information. Nevertheless, it is notable that despite the EU's strong data protection laws, the European telecoms companies had inconsistent disclosures on policies related to users' right to privacy.
While in the 2015 Index no company disclosed any data about the volume and nature of content the companies removed for terms of service violations, in the 2017 Index three companies—**Microsoft**, **Twitter**, and **Google**—received credit for revealing some data about these actions. Twitter for example disclosed in 2016 that since the middle of 2015 it had suspended over 360,000 accounts for "threatening or promoting terrorist acts."
Twitter's privacy policy was one of the clearer examples of a company explaining how it handles each type of information it collects. Still, the company did not commit to limit collection of user information to only what is necessary for the service, and did not fully disclose what information it shares with third parties.
Apple is a study in contrasts, with the highest scores for clear disclosure that it does not collect user information from third-party websites. On management of its App Store, however, Apple provided no disclosure of its processes for responding to government requests to restrict apps or the number of requests that it receives. By contrast, **Google** did provide disclosure on government requests to remove apps from Google Play.
Facebook received the lowest score of all internet and mobile companies for its lack of disclosure about how users can control what the company does with their information. More options are provided for Instagram and WhatsApp users, but only in relation to targeted advertising,
Among Chinese internet companies, **Tencent** outperformed **Baidu**, particularly for disclosing more about polices affecting users' privacy. While state secrets laws make it unrealistic to expect Chinese companies to reveal information on government requests to delete content or accounts or hand over user information, there is no legal obstacle to disclosing a range of information about how the company handles user information in the commercial context, as well the security measures it takes to protect user information.
Russian internet company **Yandex** was one of the top-performing companies for its disclosure of its security policies, but could significantly improve its disclosure of how it handles user information. This could prove material for Uber investors as Yandex has just announced an agreement to be Uber's ride-sharing partner in Russia.
Government policies have a large impact on some company scores. **Bharti Airtel** and **Kakao** scored well for disclosure on government-required grievance and remedy mechanisms. While **Bharti** is barred by the Indian government from making disclosures on specific network shutdowns, permitted disclosure on policies related to shutdowns more generally was poor.

The RDR Corporate Accountability Index analyzes a range of disclosures on issues which demonstrably influence company valuations, affecting corporate profitability as well as related asset valuations and corporate transaction values, as competition rises and users enjoy more choices about service providers. Five key findings across the Index's three issue categories—governance, freedom of expression, and privacy—are worth highlighting for their relevance to investors.

Highlight 1: Governance—A New Frontier for Boards

Digital rights issues have not generated clear norms of risk management, as highlighted by the diverse performance by companies in the Index, particularly those in the same or similar jurisdictions. Indeed, even superficially similar companies deal with digital risks in different ways. This weakness raises deeper questions about the role of board governance as boards will be expected to oversee digital rights risk management without the benefit

Figure 5 | Scores in the 2017 Index Governance Category

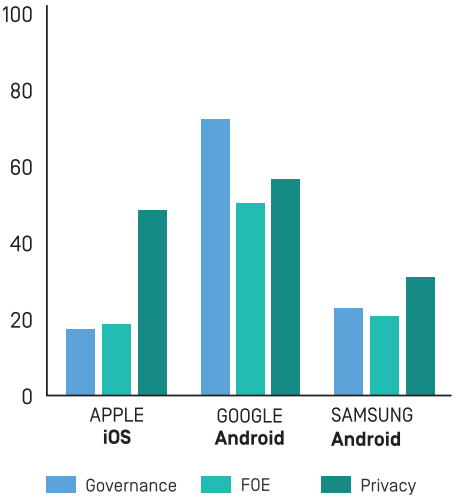


of simplistic check-lists that can be used to deflect complex oversight responsibilities. As a result, investors are well positioned to engage with company management about their digital rights risk management strategies and related board capacity.

The Governance category of the Index evaluates whether companies demonstrate that they have oversight, due diligence, and accountability processes in place to ensure that freedom of expression and privacy are respected throughout the company's operations. For a company to perform well on this category, its disclosure should at least follow, and ideally surpass, the UN Guiding Principles on Business and Human Rights as well as other industry-specific human rights frameworks focused on freedom of expression and privacy, such as the GNI Principles and the related Telecommunications Industry Dialogue (TID) Guiding Principles. Notably, GNI is a multi-stakeholder initiative whose investor constituency participated actively in the development of the initiative's governance structure and core principles. Since the release of the 2017 Index, most former TID members have joined GNI as full members. Furthermore, Index results show that companies that participate in GNI and TID tend to perform better on most governance indicators, suggesting that engagement with the issues in industry and multi-stakeholder settings can help companies develop expertise in digital risk management.

Getting board capacity right: In light of the serious risk management challenges that many companies face on digital rights issues, it should be a priority for companies to develop the board capacity required to oversee and evaluate appropriate risk management on behalf of stakeholders. Indeed, few of the boards of leading companies have professional backgrounds related to the management of complex digital rights issues. For example, this void may pose a particular challenge for companies such as Apple which underperforms its peers on key governance indicators in the Index, and also appears to lack board capacity with either the global regulatory or issue expertise investors might expect. This apparent expertise gap for Apple and others is particularly important when many companies are spending aggressively on government relations on a range of issues including the net neutrality debate in the U.S. and privacy regulations in Europe. Companies are rapidly increasing staffing levels to respond to growing demands from governments around the world concerning user-generated content, and seeking new and costly approaches to deter hackers and encrypt sensitive user data.

Figure 6 | RDR 2017 Findings on Mobile Ecosystems



Highlight 2: Mobile Ecosystems—A Black Box

As Apple's recent removal of news and VPN apps from its Chinese app store at the behest of the Chinese government demonstrates, smartphones are the new gatekeepers for digital privacy and online expression. The 2017 Index data revealed insufficient disclosure by companies of information about how their smartphones' mobile operating systems and related data services affect users' privacy, security, and access to content or specific applications. As a result, there is a persistent risk that users' legitimate expectations concerning privacy and security will continue to collide with leading companies' operating practices—and lack of disclosure about them.

For the 2017 Index, RDR evaluated three "mobile ecosystems": Apple's iOS ecosystem, the Google Android mobile ecosystem, and Samsung's implementation of Android. All three operators offered poor disclosure about policies affecting freedom of expression and privacy (**See Figure 6**). Issues of greatest material relevance to investors are:

- **Data privacy:** A key issue that the Index explores is the extent to which companies are committed to enforcing strong privacy standards for third-party mobile applications made available via the "app stores" they control. An example of this issue is Apple's recent face-off with Uber over its violation of the company's privacy rules.[7] Companies need

Users are increasingly alert to the many ways that their data is extracted and monetized by companies that choose to leave them in the dark about how this data is managed.

to demonstrate that they have clear commitments and policies in place to review and enforce privacy standards of third-party apps. No company in the Index was found to offer adequate disclosure in this regard.

- **Smartphone security:** The June 2017 "ransomware" attack that paralyzed hospitals and public facilities across the world exploited security vulnerabilities present in outdated software that had not been "patched"—or fixed through updates to the software provided by the company that makes the software.[8] Smartphones are particularly vulnerable when operating systems are not updated regularly to fix known security weaknesses. Google was the only company to disclose how long various Android device models under the company's direct control would be guaranteed to receive software updates—a "best by" date for smartphones. Samsung, which dominates the global market for Android smartphones and related devices, offers no such information to users. While other Android device makers were not included in the Index, the industry leader's failure to inform users of security risks is an example of companies passing on risk to users and investors.

As mobile becomes the dominant platform through which most of the world's users access the internet, companies that control app stores and mobile operating systems can be understood by investors to be an important chokepoint in the ecosystem of digital rights. Not only are companies like Apple, Google (via Android) and Samsung gatekeepers for how privacy and security risks are passed on to users via mobile apps, they also act as gatekeepers for other businesses seeking to reach audiences and customers via mobile apps. Apple was found to have little transparency about how it polices its app store or the number of apps it removes from app stores at the request of different governments around the world. By contrast Google published significantly more information about the volume and nature of requests it receives and responds to in relation to app removals.

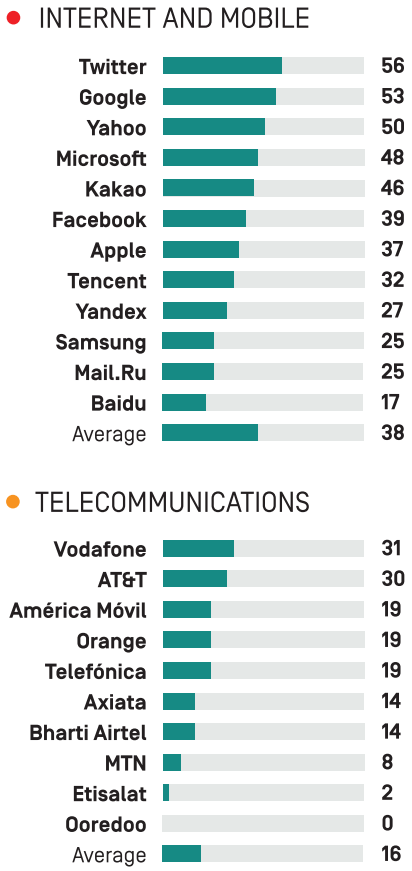
What to watch: In evaluating companies that control mobile ecosystems, investors should look for transparent policies about how security updates are managed, as well as policies about privacy and security requirements for third-party apps and the circumstances under which apps are allowed into or removed from app stores. Companies should also disclose key information in plain language about how user information is handled, an expectation for all types of companies in the sector as outlined in more detail below.

Highlight 3: User Information—The Materiality Nexus

Companies collect enormous amounts of data about their users that can be used to build profiles and track individuals. But companies also lack transparency about how and for what purpose they collect, share, and use their customers' information, and for how long they retain it. While the privacy practices of companies controlling mobile ecosystems are of growing concern, internet and telecommunications companies also generally fail to disclose enough for users to understand risks and make informed choices.

As media coverage of security breaches and privacy violations increases dramatically each year, users are increasingly alert to the many ways that their data is extracted and monetized by companies that choose to leave them in the dark about how this data is managed, whether it is kept secure, and what remedies are available in the event that problems arise. Recent published research certainly points to an erosion of user trust: The Internet Society warns that the continued rise in data breaches will not only harm individuals and damage public trust, but also could result in "lower and more selective use of the internet."[9] Roughly half of Americans surveyed in 2016 by the Pew Research

Figure 7 | Poor Company Disclosure About Their Handling of User Information



Center said they did not trust either the government or social media services to protect their data.[10] In a recent World Economic Forum survey of internet users in Brazil, China, Egypt, Germany, South Africa, and the United States, over half of global respondents agreed that user controls over the sharing of their personal information are inadequate. Less than half agreed that service providers valued users' privacy, or were reasonable in the use of their personal data. Greater transparency was rated highly as one of the key ways that companies can win users' trust.[11]

While controversy around these issues in not new, the Index is an effective tool for identifying which companies are leaders or laggards in demonstrating a commitment to protect users from unwanted breaches of privacy and security. The RDR 2017 Index found companies to be opaque about how they handle user information. While some companies disclosed more than others, none disclosed enough detail for a user to fully understand the privacy implications and potential personal risks of signing up for a service. They also gave users insufficient options to control what information is collected and shared with third parties, and few offered options for users to obtain all the information that the company holds about them.

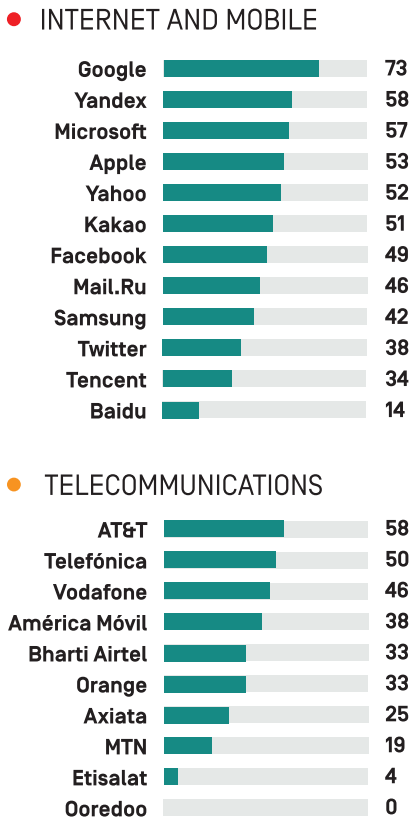
As can be seen from the bar chart in **Figure 7** depicting RDR Index scores on seven indicators addressing different aspects of how companies handle user information, these issues may be particularly relevant to broadly held companies such as Facebook, Samsung, and Apple which may be vulnerable to risk due to clear disclosure gaps.

Questions to ask: For investors interested in engaging with companies on these issues, there is a strong rationale for focusing on practical steps that companies can take to provide users with a more comprehensive picture of the lifecycle of users' personal information, from its collection to use to sharing to retention and deletion. In communicating with companies, investors should consider the recommendations for company disclosure listed in **Figure 8**.

Figure 8 | Privacy and Security Disclosure Checklist

Questions for investors to ask
1. What specific types of information the company collects;
2. How the company collects that information (e.g., does a company ask users to provide certain information, or does the company collect it automatically?);
3. Whether users have an option not to provide that information;
4. Specifically, what information the company shares and with whom;
5. Why the company shares that information;
6. Whether—and the extent to which—users can control how their information is used;
7. How long the company retains that information;
8. Whether the user can access all public- facing and private user information a company holds about them;
9. Whether and how the company destroys that information when users delete their accounts or cancel their service;
10. What are the policies for addressing security vulnerabilities, including the company's practices for relaying security updates to mobile phones; and
11. What are the policies for mitigating the risk and severity of data breaches.

Figure 9 | Disclosure of Security Policies



Highlight 4: Poor Security Disclosure Exacerbates Risk

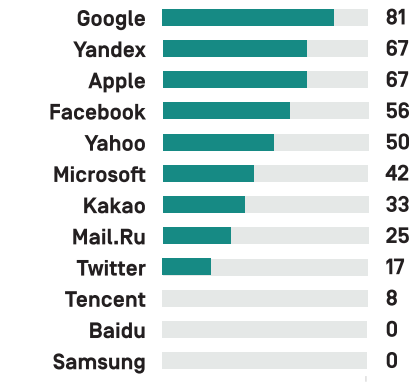
In order to trust a service, users need to know that credible efforts are being made to secure their information. In light of recent high profile hacking and ransomware incidents, investors should expect companies to provide evidence that they are making robust efforts to secure users' data. As more industries begin connecting products to the internet—from baby monitors and toys to refrigerators to automobiles—it is even more important to have credible evidence concerning the management of risks related to the interconnected networks of hardware, software, and platforms for communication and content.

The bar chart in **Figure 9** shows how companies compare on security-related questions only. Most companies evaluated in the Index communicated less about what they are doing to protect users' security than about what users need to do to protect themselves. Disclosure about policies related to responding to data breaches was especially poor.

Encryption's importance for security: One bellwether issue for investors to monitor is corporate policies and practices related to encryption. Encryption is an effective tool for protecting freedom of expression and privacy. It has a clear value proposition for users, especially those who must manage the privacy and security of their communications in an era of increasingly aggressive disruptions spanning from criminal activity to state-sponsored attacks against high-profile or high-value users. Encryption is viewed by many governments as a barrier to criminal investigations and oversight of national security threats, but many of the companies covered in the Index have resisted efforts by governments to ban or make it more difficult for companies to deploy strong encryption.[12] While the regulatory landscape around encryption remains unsettled, the value of encryption to businesses follows market demand. Of note, IBM recently announced a new mainframe—IBM Z—which can offer network level encryption reaching from local networks to cloud storage.[13] The development of these highly sophisticated new product offerings is a clear indication that regardless of the policy sensitivity, user interests are driving the development of high value new products and services to support enhanced security.

For investors to evaluate encryption policies effectively, four elements need to be disclosed: whether the transmission of user data is encrypted by default; whether data is encrypted using a unique key ("forward secrecy"); whether end-to-end encryption is used which rules out company oversight; and whether end-to-end encryption is enabled by default. Among the 12 internet and mobile companies evaluated in 2017, Google disclosed the most about its encryption policies in clear language overall, followed by the Russian internet company Yandex, which interestingly scored on par with Apple.

Figure 10 | Company Disclosure of Encryption Policies



Even for the higher scoring companies like Google and Apple, there is much room for improvement. For instance, Google does not offer end-to-end encryption in Gmail and Apple failed to disclose whether iMessage communications are encrypted with unique keys. Twitter had one of the lowest scores of all internet and mobile companies, particularly compared to its U.S. peers. For Twitter's flagship platform, users' internet traffic between their device and the company's servers is subject to robust encryption by default, but the company fails to disclose whether similar protection is offered for direct messages.

Engagement opportunity: The mixed transparency track record on encryption appears to be at odds with the technology's importance to users, especially those who are reliant on mobile and cloud based services. With this contradiction in mind, there is a clear opportunity to use a digital rights lens to engage with companies on how they perceive the legal issues and whether they will make public commitments to implement the highest encryption standards available. Moreover, with the demand for more secure services growing, it is important for investors to assess the investment and maintenance costs associated with new encrypted services. Competition around security is rising and it will be important to understand which companies have the resources and management skill to deliver these services.

Highlight 5: Freedom of Expression—Perils of Mediating Information and Content

How do company actions affect users' ability to publish, transmit, or access content? Lack of transparency about what content or user activity is or is not allowed on digital platforms can corrode consumer trust in—and therefore the value of—digitally networked products and services. With a few notable exceptions, most companies disclosed even less information about policies that affect users' freedom of expression than about policies affecting privacy and security.

Companies are struggling to handle controversies and regulatory action related to content appearing on or transmitted through their platforms and services.

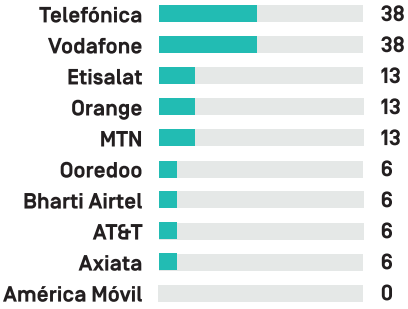
One of the perils for internet and telecom companies that play such a major role in the information economy is that companies are struggling to handle controversies and regulatory action related to content appearing on or transmitted through their platforms and services. Until recently, most of the companies in the Index did little to acknowledge the strategic challenges associated with fake news, hate speech, and terrorist content. Moreover, now that the companies are testing policies and processes to attempt to cope with the diversity of material, the policy issues for companies and regulators alike are growing even more complex and controversial.

This challenge matters because the financial reality for companies in these sectors is that the growth of user numbers and related advertising sales are key financial metrics that can define a company's growth trajectory. When a company's financial value is linked to the growth of high value users, which is then monetized through advertising, there can be an inevitable conflict between the many "communities" which catalyze the growth of user numbers and the willingness of advertisers to be associated with controversial content.[14] This situation is particularly true when the sites are home to diverse groups who often discuss controversial events, but in very different ways. As a result blunt policies around the policing of user speech and machine learning tools that are deployed to target specific controversial terms have proven to be an imperfect tool for managing risk. Efforts to solve one problem often cause new problems: take for example accusations of censorship leveled against Facebook by anti-racism activists whose accounts and postings were targeted for suspension or removal when they tried to call attention to racist hate speech.[15]

Two further issues related to online expression should be of particular concern to investors:

- **Third-party requests to restrict content or accounts:** Social media companies are wrestling with serious problems of hate speech, harassment, extremism, etc. However, the Index results revealed that companies did not disclose enough information about how they respond when governments, private organizations or even individuals ask them to block, delete, or otherwise restrict content or deactivate users' accounts. If companies are to maintain user trust and loyalty over the long run, it is important that they clearly disclose their policies for responding to and complying with requests that affect users'

Figure 11 | Disclosure of Policies Related to Network Shutdowns



ability to publish, transmit, and access information. Google, Facebook, Yahoo, and Kakao scored better than their peers on this issue, but the average score of 33 among internet and mobile companies makes it clear that there is little transparency here.

- **Network shutdowns:** Government-mandated disruption of communications networks—including shutdown of internet and mobile services and the blocking of internet messaging, social media, VOIP and SMS—are growing in frequency worldwide. Shutdowns not only affect the companies directly involved and their users; there is spillover impact across the entire sector as users lose access to email, chat, social networking, and cloud computing services which in turn has wide impact across entire economies. Sometimes shutdowns are connected with political events or security concerns. In other cases governments use shutdowns to address social concerns: several governments including India have used them to deal with students cheating on exams.[16] The implications are serious not only for citizens' ability to communicate and gain timely access to vital services (including emergency medical services), but also for business and economic activity. Yet telecommunications companies disclose very little about their policies for responding to government shutdown demands with only two companies, Telefonica and Vodafone scoring higher than 20 as illustrated in **Figure 11**.

Final takeaway: In light of recent events and controversies related to content, a key takeaway for investors from the findings of the RDR 2017 Index is that opacity increases the likelihood of underlying risk exposure. Content and access-related risks include not only blunt regulatory action, as companies now face in Germany and the UK around liability for hate speech. Risks also include reputational damage from negative media reports as well as attrition of user numbers and activity over time due to erosion of trust in growth markets or key user segments. Companies that disclose more information about how they manage information flows, access to service or content, and rules around permitted user behavior are demonstrating that they have done the hard work—internally and with external stakeholders—that is necessary to weather public controversies and respond to regulatory threats.

The Future

The RDR 2018 Index is on schedule to be released in April 2018. Because the next Index will cover the same companies with the same set of indicators and methodology as the 2017 Index, investors will be able to gain insight into which companies are making concerted efforts to improve their policies and disclosures—as well as clear visibility into which companies covered by the Index are serious about addressing their digital rights risks. The final page of this report offers a set of questions derived from the Index indicators which investors can ask of any company whose business has the potential to touch upon any aspect of users' freedom of expression, privacy, and/or security.

It is evident that user loyalty and trust in even the world's most successful platforms cannot be taken for granted: by mid-2017 younger users in the US and UK were documented to be leaving Facebook for Snap and Instagram in significant numbers.[17] The reasons are complicated and cannot be attributed to any one factor. But this trend underscores why companies need to work hard to maintain user trust and loyalty—loyalty that certainly is not bolstered when companies fail to mitigate digital rights risks that affect a critical mass of users, damaging their confidence in the products and services as well as market perceptions.

Several companies not included in the Index have informed us that they are using the Index indicators to review their own policies.

As studies point to increased consumer anxiety around digital rights issues as media coverage of controversies has grown over the past decade, a growing global movement for digital rights has emerged. In many countries, vocal users and organized advocacy networks claiming to represent user interests are also a rising force in the political and regulatory environments in which companies succeed or fail. This an important reason that policymakers as well as managers concerned with digital rights in the companies themselves pay close attention to the RDR Index results, and why several companies not included in the Index have informed us that they are using the Index indicators to review their own policies.

Meanwhile, concern for digital rights issues is moving from specialists and activists to a broader retail level. Consumer groups in the United States and elsewhere are starting to experiment with the use of evaluation frameworks to bring pressure to bear on a much wider spectrum of companies that sell products and services related to mobile applications and the "internet of things"—from smart TVs to ride-sharing apps to networked automobiles. Notably, Ranking Digital Rights is now working with Consumer Reports to refine an evaluation standard for the privacy and security of mobile applications and networked devices. RDR has also participated in exploratory research related to the digital rights risks faced by companies that provide products and services for national ID systems around the world as the organizations that help to finance these systems begin to think more concretely about due diligence and risk.

All of these intangible but powerful trends are part of the backdrop for understanding the likely trajectory of digital rights issues. Investors seeking to keep ahead of the curve will be smart to sharpen focus on digital rights issues, keeping those not currently considered material in their peripheral vision as these risks evolve with potential to influence companies' core business strategies.

Key Digital Rights Questions to Ask Companies

1. Has the company management identified digital rights risks that are material to its business and does it carry out impact assessments on the full range of these risks?

2. 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. Is the company a member of the Global Network Initiative and if not, why not?

4. 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. 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?

6. Does the company publish data about the requests it receives as well as about its own mechanisms to police user activity?

7. 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. Does the company commit to implement the highest encryption standards available for the particular product or service? If not, why not?

9. Mobile platforms: Does the company disclose clear policies about privacy and security requirements for third-party apps?

10. Telecommunications companies: Does the company disclose whether it prioritizes, blocks, or delays applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network? If yes does it disclose the purpose for doing so?

Notes

1 "Guiding Principles on Business and Human Rights" (United Nations, 2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

2 "Principles," and "Implementation Guidelines," Global Network Initiative, accessed August 31, 2017, http://globalnetworkinitiative.org/principles/index.php and http://globalnetworkinitiative.org/implementationguidelines/index.php.

3 Brian Fung, "Microsoft: U.S. government is a potential security threat," The Washington Post, December 6, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/12/05/microsoft-u-s-government-is-a-potential-security-threat/.

4 Sustainable Business Report 2017, Vodafone Group Plc, p.92, http://www.vodafone.com/content/dam/vodafone-images/sustainability/downloads/sustainablebusiness2017.pdf.

5 Darrel M. West, "Internet shutdowns cost countries $2.4 billion last year," Center for Technology Innovation at Brookings, October 2016, https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/ and ShareAction and Access Now, "Internet shutdowns: The Srisks and opportunities for technology sector investors," Investor Briefing, September 2016, https://shareaction.org/wp-content/uploads/2016/08/InvestorBriefing-InternetShutdowns.pdf.

6 Farhad Manjoo, "How to Smoke Out Where Broadband Companies Stand on Net Neutrality," The New York Times, July 13, 2017, https://www.nytimes.com/2017/07/13/business/net-neutrality-broadband-companies-fcc.html.

7 Mike Murphy, "Apple's Tim Cook once threatened to kick Uber out of App Store," MarketWatch, April 23, 2017, http://www.marketwatch.com/story/apples-tim-cook-once-threatened-to-kick-uber-out-of-app-store-report-2017-04-23.

8 Nicole Perloth and David Sanger, "Hackers Hit Dozens of Countries Exploiting Stolen NSA Tool," The New York Times, May 12, 2017, https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html.

9 "Global Internet Report 2016" (Internet Society, 2016), https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.

10 Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," Pew Research Center: Internet, Science & Tech, January 26, 2017, http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

11 "End-User Perspectives on Digital Media Survey: Summary Report" (World Economic Forum, January 2017), http://www3.weforum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf.

12 Anthony Cuthbertson, "Facebook and Google Offer no Encryption Compromise to UK Government," Newsweek, March 31, 2017, http://www.newsweek.com/tech-firms-no-encryption-uk-government-london-attack-577153.

13 IBM Press Release, 17 July 2017. https://www-304.ibm.com/jct03001c/press/us/en/pressrelease/52805.wss.

14 Mark Sweney and Alex Hern, "Google ad controversy: what the row is all about," The Guardian, March 17, 2017, https://www.theguardian.com/technology/2017/mar/17/youtube-and-google-search-for-answers.

15 Jessica Guynn, "Facebook apologizes to black activist who was censored for calling out racism," USA Today, August 3, 2017, https://www.usatoday.com/story/tech/2017/08/03/facebook-ijeoma-oluo-hate-speech/537682001/.

16 "To beat exam cheats, Gujarat to block mobile internet today," The Times of India, February 28, 2016, http://timesofindia.indiatimes.com/india/To-beat-exam-cheats-Gujarat-to-block-mobile-internet-today/articleshow/51173461.cms.

17 "Instagram, Snapchat Adoption Still Surging in US and UK," eMarketer, August 23, 2017, https://www.emarketer.com/Article/Instagram-Snapchat-Adoption-Still-Surging-US-UK/1016369.

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.