9.0 Questions for investors

The Ranking Digital Rights Corporate Accountability Index data and methodology offer a useful framework for investors to evaluate whether companies have made best efforts to mitigate risks to their business by working to anticipate and reduce potential harms to those who use their technologies, platforms, and services. Such risks are not limited to traditional "cybersecurity" threats related to hacking and data breaches. Shareholder value is also put at risk when companies fail to identify and mitigate broader risks to user privacy across their business operations, or fail to anticipate and address content-related issues spanning from hate speech and disinformation to government censorship and network shutdowns.[107]

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 key findings and recommendations from the individual company report cards.

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?

Footnotes

[107] Ben Eisen, “Facebook Stock Decline Knocks It Out of S&P 500’s Big Five,” WSJ, March 19, 2018, https://blogs.wsj.com/moneybeat/2018/03/19/facebook-stock-decline-knocks-it-out-of-sp-500s-big-five/.