The digital dilemma

The internet and social media have expanded rapidly over the last 20 years, changing many aspects of our lives. But regulation has failed to keep pace with the digital revolution, leading to social harms that pose risks for companies, investors and individuals.

Setting the scene

Over two-thirds of the global population now owns a smartphone or uses the internet.[1] The powerful internet communications and technology (ICT) sector has had significant transformative effects on nearly all other sectors and people's daily lives. But in addition to the positive impacts, such as increasing access to information and services, this has led to unexpected harms and new challenges.

These include the spreading of hate speech and the dissemination of false or misleading information, as well as violent, racist, or extremist content on social media, which can lead to devastating real-world outcomes. The commoditisation of data also creates risks to privacy rights. This has attracted the scrutiny of regulators, and poses financial, reputational and legal risks for companies and investors.

For further information please contact:

Nick Pelosi
Theme co-lead: Human Rights
nick.pelosi@hermes-investment.com

The shares of Facebook parent Meta tumbled in early February, after the company said that privacy changes made by Apple in 2021 had begun to impact its earnings. Apple's update allowed users to prevent apps from tracking their online activity for advertising purposes, impacting advertisers' ability to target specific demographics.[2] The case highlighted that as tech giants tighten up on privacy rights, social media companies that rely on harvesting individuals' data for the bulk of their income may face headwinds.

Facebook was already on the backfoot following testimony[3] given to UK and US policymakers by whistleblower Frances Haugen, who alleged that the company prioritised profitability over its real world impact.[4,5] Facebook denied the allegations, saying they were "just not true".[6] The parent company was subsequently rebranded as Meta. The company is being sued by the Texas attorney-general who alleges that it harvested and exploited biometric data without proper consent, in violation of its privacy laws. Facebook said the claims were without merit.[7]

[1] Digital Around the World – DataReportal
[2] https://www.theguardian.com/technology/2022/feb/04/meta-rivalry-apple-inflamed-facebook-parent-company-share-price-plummets
[3] https://www.theguardian.com/technology/live/2021/oct/05/facebook-hearing-whistleblower-frances-haugen-testifies-us-senate-latest-news
[4] The Facebook Files – WSJ
[5] Facebook whistleblower Frances Haugen calls for urgent external regulation | Facebook | The Guardian
[6] https://www.theguardian.com/technology/2021/oct/06/mark-zuckerberg-hits-back-at-facebook-whistleblower-frances-haugen-claims
[7] Facebook owner Meta sued by Texas over facial recognition system | Financial Times (ft.com)

Social media companies, which have grown exponentially since their humble beginnings, have not been regulated in the same way as traditional publishers and broadcasters, with disturbing consequences for Western democracy,[8] civil society[9,10] and public health.[11] Hostile state actors and violent extremists have been able to harness the power of social media platforms so that hate speech and destabilising conspiracy theories proliferate quickly.

Social media companies, which have grown exponentially since their humble beginnings, have not been regulated in the same way as traditional publishers and broadcasters, with disturbing consequences for Western democracy, civil society, and public health.

With legislators now seeking to crack down on the unfettered virtual world, companies are facing fresh regulatory risk, while reputational and financial risks are likely to grow. Companies must be prepared to balance freedom of expression with their obligations to remove problematic content while addressing government demands, laws, and regulations imposing censorship.

The UN Guiding Principles on Business and Human Rights (UNGPs) outline the corporate responsibility to respect human rights, but digital rights were nascent when the UNGPs were first published in 2011. National regulations have also significantly lagged the pace at which the digital sector has evolved, and the uses to which the technology is being put.

The UN Guiding Principles on Business and Human Rights (UNGPs) outline the corporate responsibility to respect human rights, but digital rights were nascent when the UNGPs were first published in 2011.

We have used the Ranking Digital Rights framework in our engagements with companies (see box), and have developed our own Digital Rights Principles. These build on our previous work in this area, including our white paper on responsible artificial intelligence and data governance.[12]

The principles identify the issues that ICT companies should consider when fulfilling their broader obligations to the UNGPs. We believe that companies whose business models misalign with the UNGPs have salient adverse impacts on peoples' lives and face material financial risks to long-term holistic value.

The Investor Statement on Corporate Accountability for Digital Rights

In 2021 we signed up to the Investor Statement on Corporate Accountability for Digital Rights, an initiative led by the Investor Alliance for Human Rights. This aims to tackle the online proliferation of misinformation and hate speech, increased levels of illegal surveillance, attacks on democracy, censorship of dissident voices, and discrimination of marginalised communities due to AI and algorithmic bias.

The statement outlines investor expectations for ICT companies and stresses the importance of the Ranking Digital Rights (RDR) Corporate Accountability Index. This index evaluates 26 of the world's most powerful digital platforms and telecoms companies with respect to their commitments and policies affecting privacy, and freedom of expression and information. It can be used as a tool to help companies meet their human rights and fiduciary responsibilities, and aids investors in assessing the digital rights risks in their portfolios.[13] As part of our support, we shared feedback on the RDR methodology for ranking companies, seeking indicators that enhance protections for children and young people online.

In signing up to the statement, and in our engagements, we call on companies to implement robust human rights governance, with strong board oversight, and comprehensive due diligence mechanisms that identify how freedom of expression, privacy, and user rights may be affected by the company's full spectrum of operations.

We also want companies to give users meaningful control over their data, including providing clear options for users to decide not just how their data is used, but whether it is collected in the first place, and for what purpose.

[8] Facebook appeal over Cambridge Analytica data rejected by Australian court as 'divorced from reality' | Facebook | The Guardian
[9] How The Storming of Capitol Hill Was Organized on Social Media – The New York Times (nytimes.com)
[10] Tech Tent: Did social media inspire Congress riot? – BBC News
[11] Social Media Caused the Anti-Vax Movement to Mutate. Now Tech Is Finally Fighting Back. (globalcitizen.org)
[12] https://www.hermes-investment.com/ukw/eos-insight/eos/investors-expectations-on-responsible-artificial-intelligence-and-data-governance/
[13] https://investorsforhumanrights.org/investor-statement-corporate-accountability-digital-rights

Our engagement approach

In this article we will cover three main areas – negative societal impacts, privacy rights and freedom of expression. You can read about the elements not covered here in our Digital Rights Principles.

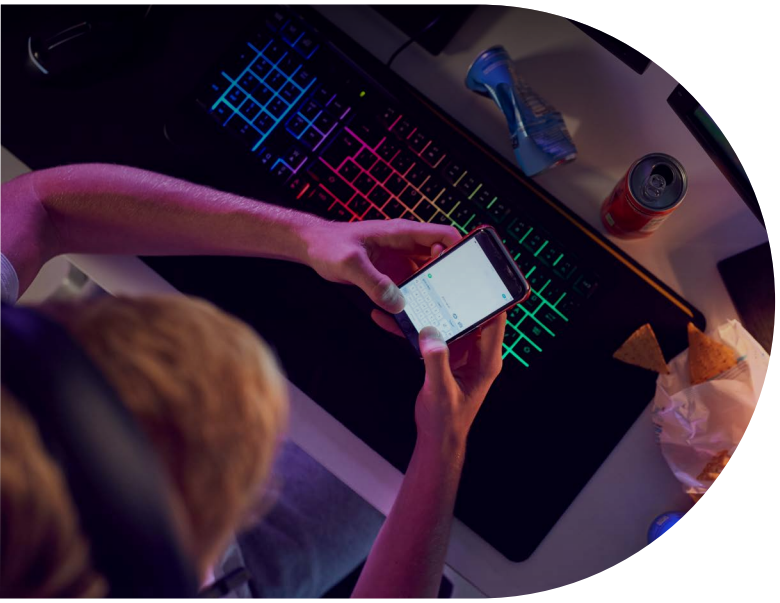
Negative societal impacts

These include problematic content on social media; misuse of artificial intelligence; health and safety impacts on children and young people; and environmental and social impacts in hardware supply chains. Companies should research negative societal impacts, be transparent about their findings and cede the appropriate authority to regulators. For example, the spread of problematic content on social media may be caused by business models correlating higher revenue with higher quantities of clicks, likes, posts, and shares.[14] Companies should not use insufficient or inconsistent regulation as an excuse for their failure to implement good practices.

Content moderation

We believe that companies should implement transparent content moderation rules on social media and report on their enforcement. In many countries, companies are granted broad powers and legal responsibilities for removing hate speech, false or misleading information, and violent, racist, or extremist content online. Companies should explain how they fulfil this role and allocate sufficient resources to personnel, including proper training and clear guiding principles.

Companies should disclose the processes and technologies used to identify content or accounts that violate the rules; report the volume and nature of the actions taken to restrict content or accounts; and offer users clear and predictable appeals mechanisms. Companies should apply more stringent standards to, and require visible labelling of, content or accounts produced, disseminated, or operated with the assistance of automated software agents (bots).[15]



Our engagement with Meta has focused on the fact that the company's business model is designed to drive hits and impressions, and on the risks related to this. While there are positive aspects to the company's products, hosting inappropriate and illegal content poses serious problems. Privacy rights are another concern.

We have set an objective for the company to conduct a human rights impact assessment for its most salient human rights issues, including emerging offerings such as the metaverse. We have encouraged the company to make its terms and conditions easier to find and understand, and to clearly obtain user consent for collection. We have also engaged with Meta in response to specific incidents. For example, we have pushed the company to be clear on how it is applying the UNGPs in reducing human rights harms and protecting human rights defenders in Myanmar.

CASE STUDY

Fujifilm

As part of our ongoing dialogue with Fujifilm, we first discussed the importance of data governance and using artificial intelligence (AI) responsibly in December 2019, highlighting the particular relevance to the company's imaging and healthcare businesses.

We said that in April 2019, the US Food and Drug Administration had published the Proposed Regulatory Framework for Modifications to Artificial Intelligence/ Machine Learning-Based software as a Medical Device paper, and shared our *Investors' Expectations on Responsible Artificial Intelligence and Data Governance* white paper. In our call with an executive officer in April 2020, Fujifilm explained its work on data governance as well as its understanding of the risks related to the use of AI. We encouraged it to document this and publish a policy.

We were pleased that the company published a Fujifilm Group AI policy following our engagement, which addresses risks such as bias, lack of fairness and discrimination and the importance of monitoring the use of AI. The policy also discusses how the company handles personal information and how it will ensure transparency and accountability, with a commitment to providing training for relevant staff. When we met again in Q2 2021, the company thanked us for our suggestions.

[14] Its-the-Business-Model-Executive-Summary-Recommendations.pdf (rankingdigitalrights.org)
[15] Ranking Digital Rights Corporate Accountability Index – 2020 indicators

Children and young people

Children and young people are vulnerable to exploitation, cyberbullying, and other risks online. We believe that companies should comply with the "safety-by-design" recommendations within the Guidelines for Service Providers set out by the OECD Council on Children in the Digital Environment.[16] These include enhanced privacy measures such as ensuring that terms and conditions are accessible to children and young people; limiting data collection to the fulfilment of service; refraining from profiling underaged users without compelling reasons; and having the appropriate safeguards in place. Companies should establish minimum age requirements for digital products and services, and report on the enforcement of protections and the percentage of revenue derived from underaged users.

We have engaged with Alphabet on data governance and privacy choices, particularly where young people are concerned. Although the company has added videos to help users understand their privacy choices on Google, in practice it is still difficult for users to give free, prior and informed consent, or to exercise control over their own, or their children's personal information. We asked the company to enhance these videos and to estimate how many of its users are underaged children and not in a position to exercise informed consent.

We have engaged with Alphabet on data governance and privacy choices, particularly where young people are concerned.

Privacy rights

The ICT sector collects, stores, and uses large quantities of data including contact information, financial information, locations, photos and videos, and web browsing activities. Data is used to provide core services and to generate additional revenue through targeted advertising and other personalised offerings. Data can be further monetised if it is shared with third parties such as data brokers that buy, repackage, and trade data for numerous purposes. Some business models depend fully on these functions, while others use data to generate revenue beyond their core purpose. The commoditisation of data creates risks to privacy rights, which may be infringed upon by governments, hackers, or the companies themselves.

Requests for information about users

Companies should maintain processes for responding to requests for information about users from governments, including law enforcement and intelligence agencies.[17] Requests may be justified in cases where authorities are seeking digital evidence against those accused of crimes, but there is a potential for misuse.

Under guidance from the Global Network Initiative, of which we are a member, companies should follow established domestic legal processes, but ensure that they screen for requests that violate basic norms or unduly infringe upon privacy rights. Where requests appear overly broad or unlawful, companies should request clarification or modification, seek assistance from outside expertise, or challenge them in the courts. Companies should keep proper records and notify individuals impacted by requests, to the extent that this is possible.[18]

We have engaged with Apple on data privacy compliance, data governance and broader human rights issues. Apple discloses data on the requests it receives from legal authorities for information about users, and for what purposes this information is sought.[19]

Many companies obtain consent by asking users to click that they agree with the terms and conditions. However, this may not meet GDPR stipulations.

User consent

Companies should obtain user consent for their own collection, inference, sharing, and retention of data. The EU's General Data Protection Regulation (GDPR) requires this of companies and stipulates that consent must be "freely given, specific, informed and unambiguous". Many companies obtain consent by asking users to click that they agree with the terms and conditions. However, this may not meet GDPR stipulations.

Companies should disclose the full range of purposes for which they collect, infer, share, and retain data, including core business purposes as well as other commercialisation purposes. In order for consent to be freely given, specific, informed and unambiguous, terms and conditions should be easy to find and understand for almost the entire user base. Written text may need to be supplemented with videos and images.

[16] OECD Guidelines for Digital Service Providers.pdf
[17] Data Beyond Borders – Mutual Legal Assistance in the Internet Age. Global Network Initiative
[18] GNI Principles Implementation Guidelines. Global Network Initiative
[19] Apple Transparency Report Privacy – Transparency Report – Apple
[20] 2020 Indicators – Ranking Digital Rights

Under the Ranking Digital Rights Corporate Accountability Index, companies score poorly in general on granting users access to and control over their data, but Alibaba receives partial credit.[20] We have engaged with Alibaba on consumer data protection and data privacy, including regarding e-payments and the sale of wealth management products (see Q&A for more details).

Freedom of expression

The Universal Declaration of Human Rights defines freedom of expression as the freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers. Technology provides unprecedented platforms for freedom of expression as well as new avenues for restrictions. An estimated 67% of internet users live in countries where criticism of governments is subject to censorship.[21]

Censorship

Companies should maintain processes for responding to government demands, laws, and regulations that impact the freedom of expression. Norms and standards inevitably vary, but companies should work with governments to develop shared understandings and promote adherence to the idea that restrictions should not be imposed except in narrowly defined circumstances.

Under the Global Network Initiative's guidance, companies should encourage governments to be specific, transparent, and consistent in their requests to restrict content or communications.

Network disruptions or shutdowns

Companies should maintain processes for responding to government orders for network disruptions or shutdowns. Such orders may be used to stop protests, censor speeches, control elections, and silence people in other ways that infringe upon the freedom of expression and other human rights.[22] The UN Human Rights Council "unequivocally condemns" such orders.[23]

Under the Global Network Initiative's guidance, such orders almost always violate the principles of proportionality and necessity. Companies should challenge governments and refrain from complying with government orders for network disruptions or shutdowns where possible, and disclose where they have complied with such orders, and for what purposes.[24]

Europe

The EU's GDPR is considered one of the world's toughest data protection laws, giving regulators the power to levy meaningful fines on companies.

For example, Amazon was hit with a €746m fine,[25] announced in its July 2021 earnings, while WhatsApp has attracted a €225m penalty.[26] The EU has also proposed two new laws – the Digital Services Act and the Digital Markets Act.[27] These aim to tackle illegal content, creating a safer space for digital rights, and to establish a level playing field for competition. Violation of the laws would attract big fines, potentially exceeding those levied under GDPR. We have signed an investor statement supporting enhanced digital rights legislation in the EU, co-ordinated by the Investor Alliance for Human Rights.[28]

In the UK, the Online Safety Bill continues its progress through parliament, and has been strengthened with new criminal offences, to tackle domestic violence and threats to rape and kill. There is academic and anecdotal evidence that misogynistic online content correlates with real world violence against women.[29,30,31] Under the terms of the proposed bill, social media companies would also be forced to stamp out the most harmful illegal content and criminal activity on their sites more quickly.[32]

For example, telecoms company Telenor, which is not in our engagement programme, discloses processes for responding to network disruptions or shutdowns, and a commitment to push back on such orders.

[21] How bad is internet censorship in your country? World Economic Forum
[22] Disconnected: A Human Rights-Based Approach to Network Disruptions | Global Network Initiative
[23] Internet shutdowns now 'entrenched' in certain regions, rights council hears | UN News
[24] Network Disruptions | Global Network Initiative
[25] https://www.wired.co.uk/article/amazon-gdpr-fine
[26] https://www.tessian.com/blog/biggest-gdpr-fines-2020/#:~:text=The%20EU%20General%20Data%20Protection,financial%20year%E2%80%94whichever%20is%20higher.
[27] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[28] Investor Statement in Support of Internet Regulations to Respect the Digital Rights of Users | Investor Alliance for Human Rights (investorsforhumanrights.org)
[29] https://journals.sagepub.com/doi/abs/10.1177/0956797620968529
[30] https://www.theguardian.com/world/2021/aug/14/plymouth-gunman-ranted-online-that-women-are-arrogant-days-before-rampage
[31] https://www.icfj.org/news/online-attacks-women-journalists-leading-real-world-violence-new-research-shows
[32] https://www.gov.uk/government/news/online-safety-law-to-be-strengthened-to-stamp-out-illegal-content
[33] 2022 will be the 'do or die' moment for Congress to take action against Big Tech (cnbc.com)

Q&A: Digital rights in China

Yu-Ting Fu
Sectors: Financial Services, Technology

In 2021 China brought in new legislation covering data privacy and data security. The Personal Information Protection Law (PIPL) is similar to the EU's General Data Protection Regulation (GDPR) and governs the collection of personal data. The Data Security Law (DSL) classifies and regulates the data that is collected and stored in China based on its potential national security impact.[34] The new legislation builds on 2017's Chinese Cybersecurity Law.

China's tech companies have expanded rapidly in recent years, mainly due to the limited restrictions on how they collect data, and on the algorithms they use.

Q. What are the aims of these new laws?

A. China's tech companies have expanded rapidly in recent years, mainly due to the limited restrictions on how they collect data, and on the algorithms they use. These new regulations will tighten up how personal data is collected, processed, stored and protected, with heavy fines for companies falling foul of the new rules.

For example, under the PIPL it is now illegal to collect excessive amounts of personal data. Also, companies are required to obtain an individual's explicit consent for the collection and use of their personal data. Authorities are obliged to investigate any complaint from consumers, and we have already seen the first legal case,[35] which was for leaking personal information on WeChat. That reached a settlement.

Q. Can you give examples of how we have engaged on these areas before?

A. We have already engaged with Chinese companies, such as Alibaba and NetEase,[36] on compliance with GDPR, so some of these areas are not new to us. These companies have established more transparent data policies and have mechanisms in place to mitigate customer grievances.

In our engagements we want to ensure that a company's approach is aligned with the requirements in the PIPL and that it is prepared to put in place responsible AI policies. We will also solicit a company's views on digital human rights, which should be fully disclosed, to reassure investors.

We suggested to Tencent that it could improve its standards further by offering more explicit information about user surveillance via methods including big data and artificial intelligence (AI).

For example, after the cybersecurity regulations came into force in 2017, Tencent made improvements to its privacy and security disclosures, providing more clarity on the underlying purpose of personal data collection and how it processes that information. We suggested to Tencent that it could improve its standards further by offering more explicit information about user surveillance via methods including big data and artificial intelligence (AI). We also suggested that it could provide more transparency on how the company implements and monitors privacy policies in offshore jurisdictions where local laws and regulations differ from Chinese legal standards, especially around human rights.

Authorities are obliged to investigate any complaint from consumers, and we have already seen the first legal case.

[34] https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws#:~:text=The%20Data%20Security%20Law%20(DSL,on%20the%20data's%20classification%20level.
[35] http://m.ce.cn/lv/fo/202109/03/t20210903_36878451.shtml (Chinese only)
[36] https://www.hermes-investment.com/ukw/eos-insight/eos/netease-case-study/

Q. What are the implications of the new data security legislation?

A. Under this law, companies must improve their data security measures and notify authorities and users of any breaches. Failures may be punished with fines, or the withdrawal of the company's operating licence. China has identified the networks and IT systems of telecommunications, energy, transportation, water, finance, public services and defence companies as critical information infrastructure (CII). Companies in these sectors are subject to much stricter data security and controls over cross-border data transfers.

Although similar requirements already exist under the 2017 Cybersecurity Law, the DSL will have a greater impact. As a result, we may encounter more resistance or hesitancy when we ask companies for more disclosure on sensitive topics.

Q. Have you seen any positive outcomes?

A. In the past, it was sometimes difficult to have a meaningful dialogue with Chinese big tech companies. However, we believe that the government's crackdown may have encouraged these companies to be more open to engagement. For example, we met Alibaba in June 2021 and January 2022. At the first meeting, the company acknowledged the need to enhance its focus on ESG and outlined plans to recruit experts and develop an ESG strategy. In January 2022 we were able to speak to a company representative appointed specifically to focus on ESG, and went into more details on the ESG strategy that the company had just launched.

During these meetings, we discussed corporate governance and shareholder engagement, human capital management, climate change, ethical AI and human rights issues. We were pleased to learn that the company had joined the United Nations Global Compact in 2021 and planned to improve its disclosure on data collection policies and processes.

We have also had useful discussions on AI ethics and data privacy with Tencent, building on the dialogue that we have had since 2015 on user privacy issues.

Many factors will have influenced these important corporate sustainability developments, including shareholder dialogue. However, we believe that the government crackdown also played a role.

Outlook

Our new Digital Rights Principles and our *Investors' Expectations on Responsible AI and Data Governance*, published in 2019, will form the basis of our engagement with the ICT sector in 2022. We want companies to apply these principles, aligned with the UNGPs, to identify and prevent the human rights risks involved in digital products and services, whilst also harnessing the opportunities that technology offers customers and communities.

In our engagements we will emphasise robust governance and policies for online privacy rights, online freedom of expression, and negative societal impacts. We will continue to liaise with other stakeholders such as the Global Network Initiative, the Investor Alliance for Human Rights, and fellow signatories of the investor statement, to advance respect for digital rights.

China has identified the networks and IT systems of telecommunications, energy, transportation, water, finance, public services and defence companies as critical information infrastructure.

Federated Hermes
EOS

Federated Hermes

Federated Hermes is a global leader in active, responsible investing.

Guided by our conviction that responsible investing is the best way to create long-term wealth, we provide specialised capabilities across equity, fixed income and private markets, multi-asset and liquidity management strategies, and world-leading stewardship.

Our goals are to help people invest and retire better, to help clients achieve better risk-adjusted returns, and to contribute to positive outcomes that benefit the wider world.

All activities previously carried out by Hermes now form the international business of Federated Hermes. Our brand has evolved, but we still offer the same distinct investment propositions and pioneering responsible investment and stewardship services for which we are renowned – in addition to important new strategies from the entire group.

Our investment and stewardship capabilities:

- **Active equities:** global and regional
- **Fixed income:** across regions, sectors and the yield curve
- **Liquidity:** solutions driven by four decades of experience
- **Private markets:** real estate, infrastructure, private equity and debt
- **Stewardship:** corporate engagement, proxy voting, policy advocacy

Why EOS?

EOS enables institutional shareholders around the world to meet their fiduciary responsibilities and become active owners of public companies. EOS is based on the premise that companies with informed and involved shareholders are more likely to achieve superior long-term performance than those without.

For more information, visit **www.hermes-investment.com** or connect with us on social media:

EOS000991 0012696 03/22.