Federated Hermes

EOS at Federated Hermes

EOS Digital Rights Principles

April 2022

For professional investors only

Introduction

Digital rights are human rights specific to digital products and services. Over two-thirds of the global population owns a smartphone or uses the internet[1]. A large and powerful internet communications and technology (ICT) sector has emerged to meet the needs of the digital revolution. The ICT sector has had significant transformative effects on nearly all other sectors as well as people's daily lives. The ICT sector's products and services play a critical role in strengthening human rights by increasing access to information and services, expanding platforms for communications and civil society, and enhancing global standards of living. They have enabled positive changes by shining a light on bad practices and elevating previously hidden issues.

The ICT sector has also brought unanticipated harms and new challenges, for example, the spread of hate speech, false or misleading information, and violent, racist, or extremist content on social media. The 2021 Facebook Files investigations accused the company of knowing that its platforms are riddled with flaws, including special privileges for elite users, toxic effects on teenage girls, and weak response to drug cartels and human traffickers. Companies must balance freedom of expression with obligations to remove problematic content as well as government demands, laws, and regulations imposing censorship. The commoditisation of data creates risks to privacy rights, which may be infringed upon by governments, hackers, or companies themselves. Meta and its social media peers are enabled by the larger network of advertisers buying their services, software companies hosting their platforms, and hardware companies building their gadgets.

These EOS Digital Rights Principles provide a high-level engagement framework for the ICT sector and other data-reliant sectors. The UN Guiding Principles on Business and Human Rights (UNGPs) outline the corporate responsibility to respect human rights, including a human rights policy commitment, a human rights due diligence process, and a process to enable access to remedy. As digital rights were relatively nascent when the UNGPs were published in 2011, these EOS Digital Rights Principles provide guidance for contemporary issues that require companies' attention when fulfilling their broader obligations to the UNGPs. 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.

[1] Digital Around the World — DataReportal

SUMMARY OF EOS DIGITAL RIGHTS PRINCIPLES

Topic	Investor Expectations
Negative societal impacts	• Ensure robust governance and policies over **artificial intelligence** • Prioritise **children and young people** in addressing negative societal impacts • Safeguard community and worker rights in **supply chains** • Take actions to close the **digital divide**
Freedom of expression	• Maintain processes for responding to laws and regulations that impose **censorship** • Implement transparent **content moderation** rules on social media • Maintain clear processes for responding to orders for **network disruptions or shutdowns** • Disclose public policy positions on **net neutrality**
Privacy rights	• Maintain processes for responding to **requests for information about users** • Maintain processes concerning **direct access agreements** • Responsible use of **facial recognition technology** • Ensure robust governance and policies over **cybersecurity** • Obtain **user consent** for their own collection, storage, and utilisation of data

Existing and emerging regulations addressing digital rights include the EU General Data Protection Regulation (GDPR) and China's proposed Personal Information Protection Law.[2] These regulations are important, but have limitations. A lack of borders online makes for complex and inconsistent enforcement that does not adhere to traditional governance models. Acceptable standards are constantly moving and companies need to regularly check in on where they benchmark. The proposed EU Digital Services Act and Digital Markets Act purports to create a safer space for digital rights and establish a level playing field.

Where relevant, these *EOS Digital Rights Principles* reference existing standards, including our EOS Investor Expectations on Responsible Artificial Intelligence and Data Governance, published in 2019; the Global Network Initiative, which establishes best practices for freedom of expression and privacy rights; and the Ranking Digital Rights Corporate Accountability Index, which ranks companies on their disclosed commitments, policies, and practices affecting freedom of expression and privacy rights. Applicable sectors include hardware (producers of cell phones, computers, semiconductors, etc.), software (internet and network services, digital content and platforms, business-to-business and cloud-based solutions, etc.), and other data-reliant sectors such as consumer goods, financial services, healthcare, and retail.

2 Personal Data, Global Effects: China's Draft Privacy Law in the International Context | New America

Negative societal impacts

The negative societal impacts of digital products and services include misuse of artificial intelligence; health and safety impacts on children and young people; environmental and social impacts in hardware supply chains; and the growing digital divide. Companies should acknowledge where their business models contribute to negative social impacts. New fields based on information sharing ("influencers") use moral codes based on real world thinking, but this is a new world where those rules might not apply. Companies should not only research negative societal impacts, but be transparent about findings and cede the appropriate authority to regulators.

1. **Artificial intelligence:** Companies should ensure robust governance and policies over artificial intelligence (AI). AI is used for numerous purposes, including by the ICT sector to curate, rank, and recommend online content, targeted advertising, search results, and political news. AI advances human development, but there is the potential for misuse. Companies could become powerful in influencing users' behaviour or contributing to social segmentation, while exerting significant control over media consumed.[3] Unintended racial, gender, and other biases have been identified within algorithms and can lead to inequitable outcomes.[4]

   Our *Investor Expectations on Responsible AI and Data Governance* provide a full engagement framework. Companies should disclose the range of purposes for which they use algorithmic systems; explain how they work, including what they optimise for and what variables they take into account; and enable users to decide whether to allow them to shape their experiences.[5] Companies should take actions to eliminate unintended racial, gender, and other biases in algorithms, including those recommended by the EqualAI Checklist to Identify Bias in AI.

   Example: Twitter's algorithmic bias bounty challenge invited the AI community to identify algorithmic bias and other potential harms.

2. **Children and young people:** Companies should prioritise children and young people, as well as other vulnerable populations, when addressing negative societal impacts. Doing so is likely to produce better outcomes for all as one in three internet users is underage. Children and youth face heightened vulnerability to exploitation, cyberbullying, and other risks online. The long-term physical and mental effects of technology on children and young people are rarely studied or explored according to UNICEF.[6]

   Companies should comply with the "safety-by-design" recommendations within the OECD Council on Children in the Digital Environment's Guidelines for Service Providers.[7] These include enhanced privacy measures such as ensuring terms and conditions are accessible to children and young people; limiting data collection to the fulfilment of service; and refraining from profiling underage users without compelling reasons and appropriate safeguards in place. Companies should establish minimum age requirements,

[3] Investor Expectations on Responsible AI and Data Governance | EOS at Federated Hermes

[4] Artificial Intelligence Has a Racial and Gender Bias Problem | Time Magazine

[5] 2020 RDR Corporate Accountability Index | Ranking Digital Rights

[6] Investigating Risks and Opportunities for Children in a Digital World | UNICEF

[7] Guidelines for Digital Service Providers | OECD

and report on enforcement of protections and percentage of revenue derived from underage users.

Example: Alphabet supplements written text in privacy policies with videos and images.

3. **Supply chains:** Companies should safeguard community and worker rights in hardware supply chains. Production of computers, smartphones, and other gadgets requires mining with significant economic, environmental, and social impacts to communities. Manufacturing takes place through complex global value chains in which labour rights violations may occur. Adverse human rights impacts may extend to end use when considering the long-term build-up of technological waste.

   Companies should require miners, manufacturers, and other suppliers to manage emissions in line with their climate change obligations under the Paris Agreement; ensure working conditions meet or exceed International Labour Organization standards; and respect local community rights, including indigenous peoples' right to free prior and informed consent. Blockchain, QR codes, and other technologies are enhancing transparency and traceability within supply chains and therefore companies' ability to address these issues.

   Example: Apple discloses processes for safeguarding community and worker rights in supply chains.

4. **Digital divide:** Companies should take actions to close the digital divide, which is the growing socioeconomic gap between those who do and do not have access to digital products and services. One-third of the global population lacks access to the internet, which is increasingly a precondition for access to finance, medicine, and other basic needs. The pandemic rendered access to the internet even more important to achieving quality education and work.

   Expanding service to urban and rural underserved populations, in cooperation with governments and civil society, should be reflected in companies' business growth and strategy, not just philanthropy. Where expanding service to underserved populations remains uneconomical, companies should provide governments with cost-per-home-passed estimates and breakeven analyses to demonstrate the impacts of subsidies.

   Example: Comcast pledges $1 billion over the next ten years to close the digital divide.

Freedom of expression

The Universal Declaration of Human Rights defines freedom of expression as 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, while only 25% of internet users have completely free access.[8] Meanwhile, the spread of hate speech, false or misleading information, and violent, racist, or extremist content online has necessitated content moderation along with responsibility on companies to define these terms. 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.[9]

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

   Under the Global Network Initiative guidance, companies should encourage governments to be specific, transparent, and consistent in their requests to restrict content or communications. Where requests appear overbroad or unlawful, companies should request clarification or modification, seek assistance from outside expertise, or challenge them in courts. Companies should keep proper records and notify individuals impacted by requests, to the extent possible.[10]

   Example: Alphabet discloses data on requests to restrict content or communications, from which legal authorities, and for what purposes.

2. **Content moderation:** 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 fulfill this role and allocate sufficient resources to personnel, including proper training and clear guiding principles as well as fair pay and mental health support.

   Companies should disclose processes and technologies used to identify content or accounts that violate the rules; report volume and nature of actions taken to restrict content or accounts; and offer users clear and predictable appeals mechanisms. Automation, outsourcing, and other cost-cutting measures necessitate additional oversight. 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").[11]

[8] How Bad is Internet Censorship in your Country? | World Economic Forum

[9] It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy | Ranking Digital Rights

[10] GNI Principles Implementation Guidelines | Global Network Initiative

[11] 2020 RDR Corporate Accountability Index | Ranking Digital Rights

Example: Meta publishes Community Standards and associated Enforcement Reports.

3. **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 freedom of expression and other human rights. The UN Human Rights Council "unequivocally condemns" such orders.[12]

   Under the Global Network Initiative 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.[13]

   Example: Telenor discloses processes for responding to network disruptions or shutdowns, and a commitment to push back on such orders.

4. **Net neutrality:** Companies should disclose if they have public policy positions on net neutrality, which is the principle that internet service providers cannot block, delay, or prioritise lawful applications, content, or websites, for any reason beyond assuring quality service and network reliability. Net neutrality rules level the field for internet traffic, but some companies oppose them as burdensome regulations that reduce access and raise costs for consumers.[14]

   Companies should disclose if they engage in practices that block, delay, or prioritise lawful applications, content, or websites, for reasons beyond assuring service quality or network reliability, including zero rating. This is when internet service providers receive fees from content providers in exchange for not charging users for the data used to access their platforms. Zero rating is criticised by net neutrality advocates for favouring content providers who can afford to pay fees.[15]

   Example: AT&T discloses an open internet policy statement that addresses net neutrality and other issues.

[12] Internet Shutdowns Now "Entrenched' in Certain Regions | UN News

[13] Network Disruptions | Global Network Initiative

[14] Pro and Con: Net Neutrality in the United States | Britannica

[15] Zero Rating: What It Is and Why You Should Care | Electronic Frontier Foundation

Privacy rights

The ICT sector collects, stores, and uses large quantities of data including contact information, communications exchange, financial information, geographic locations, photos and videos, and web browsing activities. Data is used to provide core services and often 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 companies themselves.

1. **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. Companies face growing volumes of such requests, often from numerous countries and jurisdictions.[16] Requests may be justified as seeking digital evidence against persons accused of crimes, but there is potential for misuse.

   Under the Global Network Initiative guidance, companies should follow established domestic legal processes, but ensure screening for requests that violate basic norms or unduly infringe upon privacy rights. Where requests appear overbroad or unlawful, companies should request clarification or modification, seek assistance from outside expertise, or challenge them in courts. Companies should keep proper records and notify individuals impacted by requests, to the extent possible.[17]

   Example: Apple discloses data on requests for information about users received, from which legal authorities, and for what purposes.

2. **Direct access agreements:** Companies should maintain processes concerning direct access agreements, which are legal or technical agreements that enable governments to access data in bulk, without having to submit targeted requests. Direct access agreements are often carried out with different tools and legal procedures than targeted requests, and remove companies as potential sources of scrutiny, transparency, and accountability from government surveillance activities.

   Companies should challenge direct access agreements and refrain from entering them, where possible. Where direct access agreements are required or unavoidable, they should be authorised in clear, easily accessible, and understandable laws, and accompanied by explicit transparency, oversight, and accountability measures.[18] Companies should disclose if and where they have entered direct access agreements, and for what purposes.

   Example: The Telecommunications Industry Dialogue states that "governments should not conduct any type of registry, search, or surveillance by means of direct access to companies' infrastructure without any technical control by the company."

3. **Facial recognition technology:** Companies should deploy Facial Recognition Technology (FRT) responsibly. Companies and governments alike are quickly adopting FRT for a variety

[16] Data Beyond Borders – Mutual Legal Assistance in the Internet Age | Global Network Initiative

[17] GNI Principles Implementation Guidelines | Global Network Initiative

[18] Defining Direct Access | Global Network Initiative

of security and efficiency purposes. However, human rights risks include racial and gender biases observed within algorithmic systems; questionable accuracy and lack of public testing; possible privacy or legal violations in the sourcing of photos for databases; and misuse by some governments, law enforcement agencies or others.[19]

Under the Investor Statement on Facial Recognition, companies should disclose the accuracy of their technology after measurement by a recognised and relevant scientific assessment institution; disclose the sources of their image databases and demonstrate that their technology is constantly monitored to detect algorithmic biases, particularly with respect to race, gender, or age; demonstrate proper due diligence of clients before making the technology available to them; and demonstrate that effective grievance mechanisms are in place to enable victims to report consequences and to access remedies.[20]

Example: IBM discloses policies on FRT opposing use for mass surveillance, racial profiling, and violations of basic human rights and freedoms.

4. **Cybersecurity:** Companies should ensure robust governance and policies over cybersecurity. The scale and frequency of breaches continues to rise, and the World Economic Forum consistently ranks cybersecurity as one of the top five risks to businesses. Breaches can cripple business operations, create legal and regulatory risks, and have adverse human rights impacts.

   US-based law firm Wachtell, Lipton, Rosen and Katz states that boards should not be involved in day-to-day risk management but should have oversight mechanisms informed by sufficient expertise. Response strategies should cover all categories of likely scenarios, as well as unlikely but plausible scenarios with extreme consequences. Appropriate and compliant disclosure should be made if systems are materially compromised.[21]

   Example: The PRI evaluates cybersecurity disclosure against 14 indicators while the US National Institute of Standards and Technology develops standards, guidelines, best practices, and resources for US industry.

5. **User Consent:** Companies should obtain user consent for their own collection, inference, sharing, and retention of data. The EU's GDPR requires companies to do so and stipulates that consent must be "freely given, specific, informed and unambiguous". Many companies obtain user consent by having users check the terms and conditions. However, this may not constitute consent that is "freely given, specific, informed and unambiguous".

   Companies should disclose the full range of purposes for which they collect, infer, share, and retain data, including core business purposes as well as additional 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 close to the entire user base, which may require supplementing written text with videos and images. Companies should take actions to grant users heightened access to and control over their data.[22]

   Example: Under the Ranking Digital Rights Corporate Accountability Index, generally companies score poorly on granting users access to and control over their data, but Alibaba receives partial credit.

[19] Investor Statement on Facial Recognition. Candriam

[20] Investor Statement on Facial Recognition. Candriam

[21] Cybersecurity Oversight and Defense — A Board and Management Imperative. Wachtell, Lipton, Rosen and Katz

[22] 2020 Indicators - Ranking Digital Rights

For professional investors only. The activities referred to in this document are not regulated activities. This document is for information purposes only. It pays no regard to any specific investment objectives, financial situation or particular needs of any specific recipient. Hermes Equity Ownership Services Limited ("EOS") and Hermes Stewardship North America Inc. ("HSNA") do not provide investment advice and no action should be taken or omitted to be taken in reliance upon information in this document. Any opinions expressed may change. This document may include a list of clients. Please note that inclusion on this list should not be construed as an endorsement of EOS' or HSNA's services.
EOS has its registered office at Sixth Floor, 150 Cheapside, London EC2V 6ET. HSNA's principal office is at 1001 Liberty Avenue, Pittsburgh, PA 15222-3779. Telephone calls may be recorded for training and monitoring purposes.