INVESTOR ALLIANCE FOR HUMAN RIGHTS

Sector-Wide Risk Assessment of Information and Communications Technologies

# PRIVACY AND DATA PROTECTION

The digital collection of personal data can generate significant economic and social benefits such as reducing security risks and facilitate the provision of goods and services online, however, it can also have a detrimental impact on fundamental rights, including the right to privacy.

## *International standards*

*The following are some of the main international instruments that refer to privacy and data protection that companies must consider when conducting human rights due diligence.*

Although international human rights law provides the universal framework against which any interference with privacy must be assessed, in December 2013 the UN General Assembly addressed the right to privacy in the digital age, making clear that it should be protected both *online* as well as *offline*. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights state that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Privacy is considered a gateway right that enables the realization of other rights, including the rights to life, liberty, and security of person (Article 3), the right to freedom of opinion and expression (Article 19), and the right to freedom of peaceful assembly and association (Article 20). Other relevant standards can be found here.

## *Salient privacy issues to consider when engaging with ICT companies*

*The concept of 'salience' focuses on risk to people, not to the company, while recognizing that where risks to human rights are greatest, there is significant convergence with business risk.*

ICT companies can negatively impact the right to privacy in a number of ways, including by: I) Failing to protect the confidentiality of personal data of users, employees, customers or other individuals; II) Requesting user data while providing unclear or misguiding information on how it will be used; III) Inappropriately using individual's personal data without their knowledge or consent to make predictive analyses that inform decision-making; IV) Tracking individuals' movements and physical location without their knowledge by enabling online location services; V) Providing private user information to State authorities in response to requests that are illegal under national law and/or not in line with international human rights standards; and by VI) Selling technology equipment to governments with poor human rights records that are used to track or monitor individuals' communications and movements.

### Resources

The Global Network Initiative (GNI) brings together companies, investors, civil society organizations, and academics in an effort to protect privacy when confronted with government demands, laws, or regulations that compromise privacy.

United Nations Special Rapporteur on the right to privacy.

Sharing.Data Guidance, aims to set out good practice in data collection and management to enable data sharing in compliance with the relevant legislation.

Report of the OHCHR on the right to privacy in the digital age, clarifies principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business.

10 things to know

Unjustified or arbitrary limitations to the right to privacy can also lead to a wide range of adverse impacts on other human rights, including liberty and security (e.g. persecution and even death of activists); freedom of opinion and expression (that includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers); democratic participation (e.g. exploitation of user information for political purposes); and non-discrimination. More detail on other impacts can be found in other sections of the assessment.

The 2018 'Ranking Digital Rights (RDR) Corporate Accountability Index' found that online users remain largely in the dark about what information they are sharing, with whom, or for what purpose. Such information can be shared with third parties, including governments, courts, and law enforcement who make legal demands for user data, as well as with advertisers. RDR has also established that detailed profiles created with users' information can be used by government agencies to identify surveillance targets, financial service companies to determine creditworthiness, and businesses and other organizations (including advocacy groups and political campaigns) to target people with advertisements and marketing campaigns tailored to their profiles.

## *How does Artificial Intelligence impact the right to privacy?*

The rapid development and use of Artificial Intelligence (AI) related technologies poses several risks to human rights, including the right to privacy. For instance, AI-driven consumer products and autonomous systems (e.g., automated online assistants), generate and collect vast amounts of data without the knowledge or effective/informed consent of the users. There are also concerns over the privacy impacts of facial recognition software and the effects of some 'predictive policing' methods.

AI-driven applications are used to automatically sort, score, categorize, assess and rank people, often without their knowledge or effective/informed consent, and frequently without the ability to challenge the outcomes or effectiveness of those processes. A recent report by the Office of the High Commissioner for Human Rights, pointed out a widely shared concern of algorithmic discrimination and bias on AI-systems, and warned of the disproportionate and disparate impacts of AI on certain groups facing systemic inequalities, in particular women.

INVESTOR ALLIANCE FOR HUMAN RIGHTS

# *The 'Business Case' for privacy and data protection*

*Beyond their human rights responsibilities, ICT companies that do not proactively assess and address privacy risks face potential legal, reputational, and financial risks.*

Today, businesses of all sizes are recognizing that privacy and data protection are a vital competence driven by evolving regulations around the world and the increasing material risks resulting in reputational harm, financial loss, regulatory actions and fines, shareholder lawsuits and dissatisfaction among customers and users. In 2016, a US survey found that high-profile data breaches negatively impacted consumer trust in major brands, with 76 per cent of respondents stating they would likely take their business elsewhere due to negligent data handling practices, while 72 per cent of consumers said they would share far fewer personal details with companies in light of recent privacy breaches. To prevent these risks, there are a number of **key points for companies** to consider:

| | | |
|---|---|---|
| **Develop and implement appropiate policies and due diligence procedures to safeguard privacy and data protection** | Ensure there is a clear connection to the company's human right policy commitments; | |
| | Adhere and implement the **GNI principles** on privacy: | Employ protections with respect to personal information in all countries where they operate in order to work to protect the privacy rights of users. |
| | | Respect and work to protect the privacy rights of users when confronted with government and state authorities' demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards. |
| | Produce operational guidance and training for specific company functions, such as information technology, product or service development, sales and marketing and human resources; | |
| | Tell users whether and how they are tracked in real time through simple, understandable and concrete information. Companies should clearly disclose whether and how they collect user information from third-party sites and services in real time; | |
| | Information and metrics that are provided to the board, must include a cyber security strategy, threat assessments and resulting impact on company (reputational, financial, etc.), data analytics to limit risk, staff awareness, training and assurance; | |
| | As employees and customers are commonly cited as high-risk factors, it is important to promote awareness of the importance of cyber security for users, including developing training modules on privacy and data protection; linking employees' performance and bonuses to their addressing privacy risks; hiring internal or external experts to build curriculums on cyber security and data privacy; | |
| | Invest in the development of technologies and business models that maximize user control over their personal information and content - respect and protection of privacy by design. | |

INVESTOR ALLIANCE FOR HUMAN RIGHTS

# *Investor guidance for engaging ICT companies on privacy and data protection*

*Shareholder value is at risk when companies fail to identify and mitigate broader risks to users' privacy across their business operations. The following questions - based mainly on the RDR index and the RDR Investor Update 2018 - are intended as a starting point for investors engaging with ICT companies to help them evaluate if companies are making adequate efforts to protect data and respect the right to privacy.*

- Does the board exercise direct oversight over risks related to users' security/privacy? Does board membership include people with expertise and experience on issues related to privacy rights?
- Does the company conduct ongoing human rights due diligence to identify real and potential adverse impacts associated with operations in consultation with stakeholders, including independent human rights experts?
- 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?
- Does the company take any kind of measures to anticipate and mitigate any negative impact that their products, services, and business operations may have on users' right to privacy?
- In case of any type of violation or restriction on users' rights to privacy and data protection, does the company guarantee users' access to appropriate public and/or private remedies, including effective and accessible grievance mechanisms?
- 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 and internet companies)? Does the company apply additional due diligence where requests are made by state authorities in countries that receive particularly low rankings in civic/political freedom indices and/or are considered conflict-affected areas?
- Does the company disclose clear information about policies for addressing security vulnerabilities, including the company's practices for relaying security updates to mobile phones?
- If the company operates mobile ecosystems, does it publicly communicate clear policies about privacy and security requirements for third-party apps?

## *Investor Efforts*

*Investors are taking steps to prevent and mitigate human rights and material risks, and hold ICT companies accountable for adverse human rights impacts. Here are some examples:*

- ✓ Investor Alliance of Human Rights Statement in support of Ranking Digital Rights Corporate Accountability Index.
- ✓ Facebook's largest shareholders urged to hold the company accountable
- ✓ Investor-company dialogue on cyber security: five emerging findings
- ✓ Global fintech investors team up to promote responsible digital finance, which includes establishing Customer Identity, Data Privacy and Security Standards

---

*Developed by the **Investor Alliance for Human Rights**.*

*We would like to thank **Global Partners Digital**, **Access Now**, **Open Mic** and **Heartland Initiative** for their input in the development of this module.*