



Buffering rights

HOW EUROPE'S NEW DUE DILIGENCE REGULATION CAN HELP REVERSE TECH RIGHTS RISKS

Executive summary

The current technology revolution has enormous potential for human development: to enhance democracy, safeguard human rights and increase transparency within our society to combat inequality. But the dark side of technology has been growing quickly: hate speech, fake news, intrusive surveillance, coercive algorithms, discriminatory artificial intelligence (AI) and pollution. Currently, without adequate business regulation, inscrutable and abusive practice by irresponsible tech companies can enjoy impunity. The existing scale and scope of abuse risks squandering public trust in the tech giants for good, permanently endangering their social licences to operate – and to help fulfil the promise and progression a responsible tech industry could and should deliver.

Europe's welcome draft Corporate Sustainability Due Diligence Directive (the Directive) seeks to transform the European business model by stipulating that companies must undertake human rights and environmental due diligence (HREDD) to assess risks and harms in their global operations and supply chains. This must ultimately lead them to take action to prevent, eliminate or mitigate these risks. The Directive has enormous potential to insist the tech sector transforms itself to end abuse, and contributes to shared prosperity and effective democracy. This represents a significant step forward for corporate accountability in advancing the mandate of international frameworks like the United Nations Guiding Principles on Business and Human Rights (UNGPs), and may also act as a precedent for other jurisdictions.

This briefing explores the extensive implications of an improved Directive for the tech sector. We highlight how the Directive can reshape the sector's contribution to society while identifying weaknesses which must be addressed for the Directive to deliver on its full potential. With partners and allies from across the world, we have developed specific recommendations which will allow the Directive to support greater human rights

and environmental protection, deliver on the intentions of the European Union and create a more level playing field for responsible tech companies. In so doing, the Directive could also go some way to help restore public trust in an increasingly discredited sector by changing the calculus of risk in tech company boardrooms to consider the human rights and environmental responsibilities of this critical sector. The good news is this task is relatively straightforward.

The Directive is built on the UNGPs, and bringing the Directive fully in line with them will address its primary weaknesses relating to its application to the tech sector. Many of the areas for strengthening the Directive have already been identified by civil society, legislators, responsible companies and investors – and these are the same elements that will make the Directive powerful in transforming the tech sector. Our analysis also provides the tech and rights movement with another compelling set of arguments from an under-analysed corporate sector for their reform proposals to the European Commission.

First, the threshold for companies covered under the directive, in relation to their size and turnover, needs to be revised and significantly lowered. At a minimum, the tech sector needs to be included in the Directive's list of high-risk sectors. Many high-impact tech companies, especially those providing surveillance or facial recognition software (among others), would be omitted from the Directive's ambit under its current drafting, despite their profound potential for human rights impact. In light of this potential, with significant risk of discrimination and abuse at work and play, the Directive needs to also be clearer about the full scope of human rights and environmental damage that is covered, in line with the UNGPs.

Second, the tech sector is often characterised by the sporadic nature of contracts that, despite their transience, have profound human rights implications. This includes facial recognition technology, which typically begins with a coding process by one firm (or even individual) and develops over time through other partnerships and relationships. The Directive therefore needs to prioritise the UNGPs' principle of due diligence and should cover the whole value chain, with a focus on severity of risk and impact replacing its current focus on "established business relationships", which allows for impunity in the face of harmful supply chains.

In the tech sector especially, stakeholder engagement lies at the centre of effectively determining these risks. Without stakeholder engagement, 'user-friendly' has too often morphed into 'user-abusive'. The Directive needs to transition from characterising stakeholder engagement as an option in the process of identifying and addressing human rights risks, to being the mandatory centre of effective corporate due diligence. Protection for the rights of those stakeholders who come forward for engagement – including those who may deliver some hard truths to the sector, such as human rights defenders – should be included in the Directive without reservation.

Finally, the Directive's inclusion of a complaints procedure, penalties and civil liability contributes to a robust approach to protecting human rights and the environment and can help develop a level playing field for responsible companies and investors. However, these need to be strengthened to remove barriers. To ensure the effectiveness of civil liability in the tech sector, the Directive needs to insist on less opacity so victims can gain access to key information. The burden of proof should be with the company to demonstrate it has acted lawfully on due diligence, rather than on the victim to show that the company has not.

In sum, this briefing demonstrates that an effective European due diligence law would help transform the tech sector's all-too-frequent response to human rights abuse – from 'how could we have known?' to a proactive 'how do we know (and act)?'. This shift is within reach.

Introduction and background

As part of its [Sustainable Corporate Governance](#) initiative, the European Commission published a [legislative proposal for Corporate Sustainability Due Diligence](#) in February 2022. The Directive seeks to create a framework for comprehensive human rights and environmental due diligence to be carried out by companies. The proposal builds on the foundation set out in the UNGPs on due diligence, corporate responsibilities and human rights. This Directive is the first regional attempt to mandate comprehensive human rights and environmental due diligence, whereby companies must identify, prevent and mitigate these actual and potential risks and impacts in their operations and value chains, and to include administrative penalties and civil liability where companies fall short. It is an important step for corporate accountability, which has prompted [widespread analysis](#) to date.

In relation to the technology sector specifically, the Directive should be welcomed as a much-needed innovation with the potential to help address the risks the sector presents to tech users and society at large. This is critical: recent illustrative examples of tech-related harms have included:

- ➔ The [weaponisation of hate speech](#) causing online and offline rights violations;
- ➔ Illegal [surveillance](#) resulting in loss of privacy;
- ➔ [Censorship](#) of political dissent impeding freedom of expression;
- ➔ Biases being [built into AI](#) and automated decision-making processes further marginalising vulnerable communities; and
- ➔ The [dumping of e-waste](#) without adequate refurbishment of the environment.

These cases highlight tech-related harms which can extend to both users and non-users of technologies and are typically felt most severely by already-vulnerable groups. Tech companies can play various roles in these infringements, from directly contributing to abuse to creating technologies used to cause harm by those far beyond a firm's "first-tier" customers. The impacts of a particular piece of technology may also shift over time. Therefore, decisions taken by tech companies across a product's life cycle – including during product design, promotion, deployment, selling and licensing, and oversight of use – provide [fertile ground](#) for human rights harms.



Mandatory human rights and environmental due diligence has a critical role in limiting the negative impacts of an industry with extraordinary potential for societal harm. The recent example of telecommunications company Telenor, which undertook a human rights impact assessment as part of its due diligence before entering the Myanmar market, meant the company was in a position to make informed decisions when faced with the rapidly escalating conflict situation, is instructive. It stands in stark contrast to the alleged approach by Facebook, now Meta, which failed to undertake due diligence relating to its operations in Myanmar and was [widely criticised](#) for failing to act against harmful content on its platform calling for violence against the Rohingya.

The Directive has the potential to build on other EU regulatory efforts already underway which specifically address challenges related to the tech sector, including the proposed [Digital Services Act and the Digital Markets Act](#). By mandating effective due diligence, the Directive could contribute to these endeavours to democratise and make available accountable technology for all – with direct impacts for both EU and non-EU constituents, and potentially serve as a reference point for other jurisdictions.

An added benefit for companies would be a reduction in reputational and financial risks, plus the avoidance of legal risks stipulated in the Directive. A robust and predictable HREDD framework, including legal consequences where firms fall short, should help create a level playing field for companies, increase certainty around the operating environment for those companies and their investors, and improve human rights practices across the sector. The following analysis provides a roadmap for clarifying and sharpening the text of the Directive in order that it can achieve these aims.

Strengthening the Directive to fully address human rights and technology

The Directive will directly apply to both EU and non-EU tech companies that meet certain thresholds, and will likely have broader, global implications through the 'Brussels Effect' (by which international companies often adopt European regulatory standards, even where not compelled, in order to simplify their supply chains and operations). Therefore, it is critical to ensure the Directive is sufficiently well designed to improve responsible practice in this high-risk sector. With partners and allies across the world, we have identified the following key areas where strengthening the Directive will support far greater human rights and environmental protection in the context of the tech industry, deliver the intentions of the European Union, create a level playing field for responsible tech companies, and rebuild the sector's lost social licence to operate.

Key areas to improve:

-  [Scope of companies and sectors](#)
-  [Scope of rights](#)
-  [Value chains and business relationships](#)
-  [Stakeholder engagement](#)
-  [Complaints procedure](#)
-  [Liability](#)

Scope of companies and sectors

Many tech and digital companies employ relatively few people, yet have profound human rights and environmental impacts. Companies providing surveillance tech or facial recognition software, for example, may have a [limited number of people](#) on payroll, but the consequences of these types of technology, especially for human rights defenders and journalists – guardians of open and robust democracy – can be substantial.

Purportedly to avoid onerous regulation of small enterprises, the Directive was drafted to apply to companies formed in accordance with the legislation of an EU Member State, that meet certain thresholds – generally measured by number of employees and turnover.¹ Importantly, part-time and temporary agency workers, both common in the tech sector, are included in the definition of ‘employee’ as per Article 2(3). Companies with more than 500 employees and a net turnover of €150 million would be subject to the law as a matter of course. A welcome lower threshold says the Directive also applies to smaller companies that have over 250 employees and a net turnover of €40 million, but which operate in specified “high-impact sectors”.

Unfortunately, neither technology nor digital industries are included in the list of “high-impact sectors”, which is a critical oversight. The Directive will be far more effective if these sectors are included, which would ensure substantially more tech companies are required to perform at least some human rights and environmental due diligence.

However, even for those sectors currently included in the Directive’s “high impact sectors”, companies are only required to identify and address their severe impacts “relevant to the respective sector”, rather than to undertake a [broad, risk-based approach](#) to due diligence contemplated by the UNGPs. In relation to the tech sector, even if it is eventually included in this list, this approach is problematic. Given the rapidly evolving nature of the diverse impacts of technology, this provision must be revised in line with the UNGPs, even if technology is eventually included in the list of “high impact sectors”.

Recommendations:

- ➔ The Directive should be amended to apply to all EU-operating companies, with a specific understanding that while the responsibility to respect human rights and the environment applies to all businesses, the means through which a company meets the required standards will vary according to size and severity of impacts, among other factors.
- ➔ At a minimum, technology should be added to the list of high-impact sectors and all thresholds should be lowered to bring the Directive in line with the UNGPs in relation to the responsibility of all companies to respect human rights.
- ➔ All companies covered by the Directive should be required to undertake the same broad-based approach to due diligence as provided for in the UNGPs, including those covered by the Directive through their classification as “high impact” sectors and currently subject to more limited due diligence requirements.

¹ See also Article 2 of the Directive, describing applicability of the Directive to companies formed in accordance with legislation of a third country, and including only turnover thresholds, regardless of number of people employed.

Scope of rights

The material scope of the Directive refers to the range of rights it covers, set out in [Annex 1](#), which stipulates that companies must assess and address adverse impacts on people and the planet resulting from a “violation” of those rights, obligations and prohibitions. Annex 1 specifies that violations of rights not specifically listed therein, but included in certain international human rights agreements referenced in Annex 2, may be covered by the Directive, where the company concerned could reasonably have established the risk associated with impairing the right and taken appropriate measures.

Many key rights which can be heavily impacted by tech companies have not been explicitly mentioned in the text. Most critically, the current list does not include the right to freedom of expression. The general right to be free from discrimination on the basis of race or gender has also been excluded, despite increasing evidence certain technology affects minorities and marginalised populations unequally. The rights to health and to education are also not mentioned. Both are increasingly directly impacted by technology, as seen in discourse on the [mental health impacts](#) of social media platforms and growing digitisation of school education that risks leaving behind those without internet access.

The fact only a limited number of human rights are specified, whereas other key rights are possibly covered by the ‘catch-all’ of Annex 2, creates ambiguity and possible contradictions with the international human rights standards of the UNGPs. This may lead companies to narrow the scope of human rights considered covered by the Directive or to read a hierarchy of rights into the legislation. Further, given that rights impacts of tech companies – as with other companies – can evolve over time, a more inclusive approach to rights covered in the instrument would strengthen the Directive.

The Directive would also be bolstered by a more deliberate acknowledgment of the intersectional impact of rights: for instance in tech value chains, where women migrant workers are at highest risk through gender, racial and class discriminations. The Directive will lend far greater protections in the tech sector if companies’ impacts on gender and vulnerable groups are highlighted as specific points of analyses in HREDD.

Recommendations:

- ➔ The list of rights enumerated should be expanded to include those often impacted by technology, such as freedom of expression. It should be made clear this list is non-exhaustive. Alternatively, the Directive could be strengthened by making it clear due diligence obligations extend across the full spectrum of rights enumerated in an expanded range of international human rights instruments, in line with the UNGPs, rather than including a list enumerating some rights.
- ➔ The Directive should explicitly require companies to examine the intersectionality of rights and contexts of marginalisation. This should include requirements for companies to consider their impacts on marginalised groups and apply a gender lens in the HREDD process.

Value chains and business relationships

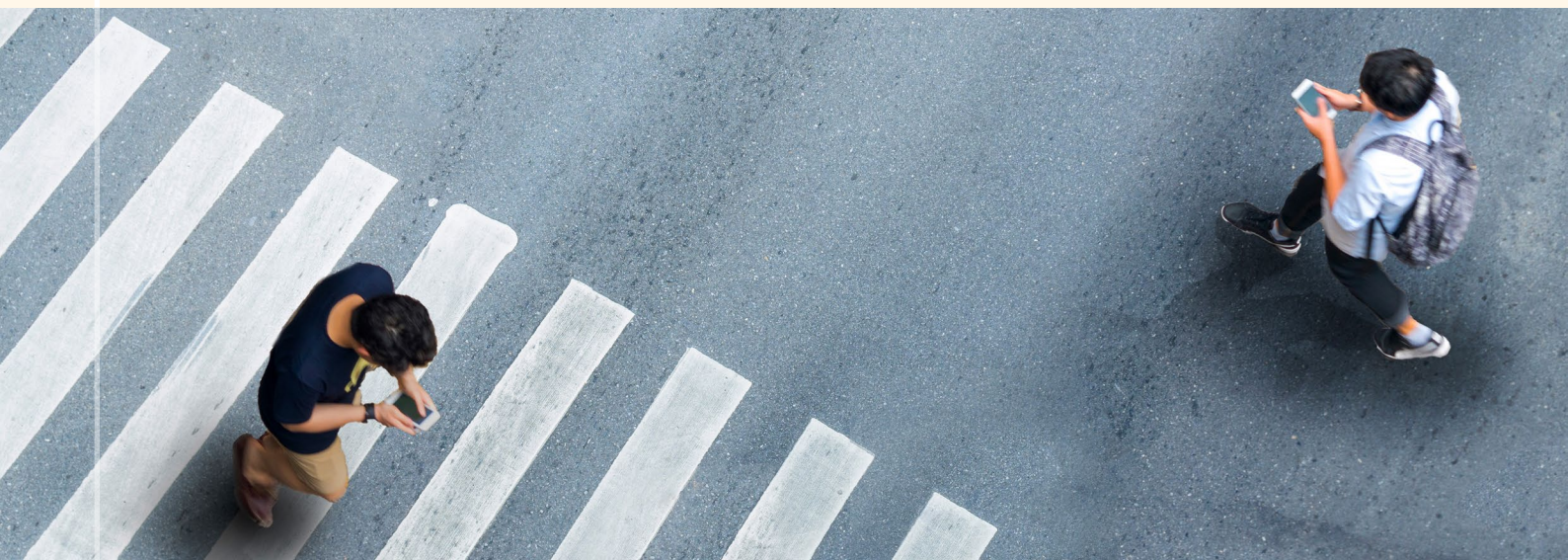
In line with the UNGPs, the Directive requires companies to conduct HREDD with respect to their own operations, their subsidiaries and their value chains. Currently, article 1(g) defines “value chain” as “activities related to the production of goods or the provision of services...as well as related activities of the company’s upstream and downstream ‘established business relationships’”. The recognition of upstream and downstream value chains in this provision is welcome to help address the full rights impacts of the tech sector, but the limitation to “established business relationships” – defined in terms of intensity or duration, as provided in Article 1(f) – may undermine its effectiveness.

The downstream value chain affects the lives and rights of millions of tech users and non-users. These assessments are therefore critical in assessing “[the human rights impacts that occur during and after the sale of a product or service and are influenced by the business inputs to that product or service.](#)” The procurement, deployment and experience of AI and surveillance technology provide a case in point. For example, AI deployed by police has been [shown to drive racial discrimination](#), and Uber drivers have been [dismissed from their jobs](#) without explanation due to coercive and opaque algorithms.

In the tech sector, business relationships with major human rights implications are often transient and sporadic. For instance, a major tech company may be contracted to develop codes at different points that will form part of a comprehensive worker surveillance tool, impacting gig and service workers, with implications for their welfare. But the developer company may well not define this relationship with the buyer, ultimately producing a comprehensive worker surveillance tool as an “established business relationship”. Similarly, technology may be sold to a government through a single contract while the company continues to upgrade or troubleshoot said technology, without this qualifying as an “established business relationship” under the Directive. In line with the UNGPs, the Directive should focus on the principle of severity of risk, rather than the longevity of a business relationship to guide the due diligence requirement.

Recommendation:

- ➔ The Directive should explicitly require companies to extend their due diligence across the full value chain, and cover all business relationships, irrespective of their duration or intensity, defined instead through analysis of actual or potential harm and salient impact.



Stakeholder engagement

Stakeholder engagement is vital to sustain the tech sector's licence to operate. The collapse of public trust in tech giants is perhaps primarily rooted in the growing perception companies have failed to take people's concerns and rights into account as they have developed revenue models that appear to have baked-in abuse of freedoms and dignities.

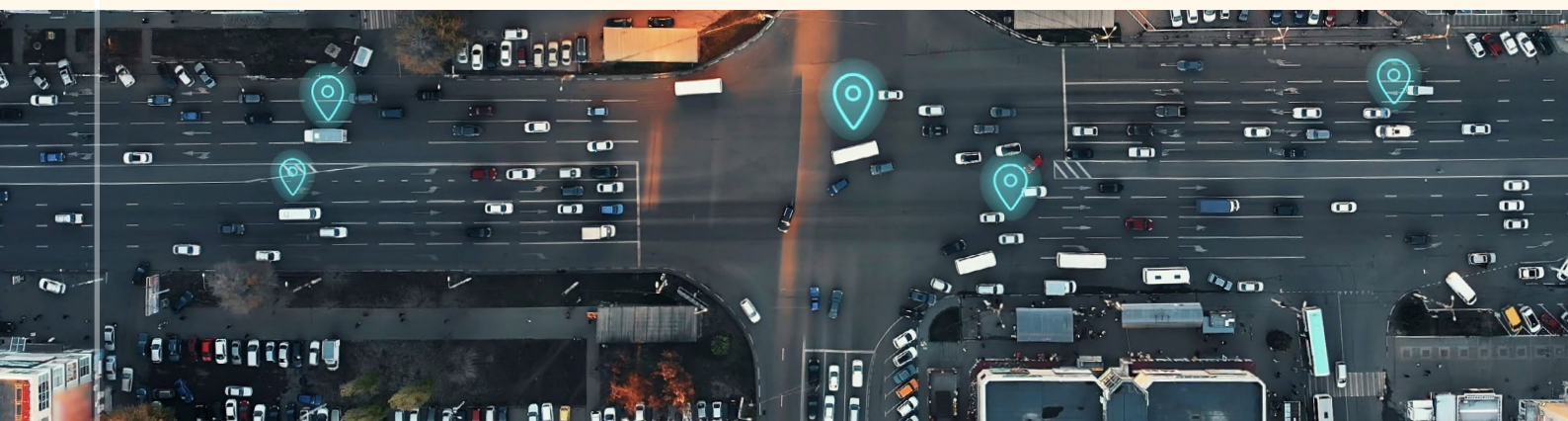
Article 6(4) of the Directive mandates that companies, where relevant, may carry out consultations with potentially affected groups, including workers and other relevant stakeholders, to gather information on actual or potential adverse impacts. Stakeholders are narrowly defined in Article 3(n) to mean employees and other potentially affected individuals, groups, communities or entities, and the Directive does not suggest precautions must be taken to ensure protection for participants in such engagements. These are areas for improvement.

First, this provision is drafted in a manner to suggest stakeholder engagement may be 'optional', whereas it should be unequivocally required for the tech sector to identify risks. The quality of human rights due diligence improves significantly when it draws upon insights from a wide range of stakeholders, including professional communities which hold critical, technical or social knowledge, and affected groups – especially women and marginalised communities. Tech companies should employ a “[human rights by design](#)” approach in their work, based on substantive engagement with stakeholders, to enhance the protection of human rights. With this, technology has a real chance of being welcomed as beneficial, aiding human development. Without it, there is danger of abuse and resistance.

Further, effective stakeholder engagement, as envisioned by the UNGPs, must be both safe and meaningful. Tech companies will need to be more transparent to ensure informed engagement by stakeholders through access to data and information. Whistle-blower protections and anti-retaliation policies are needed to avoid intimidation which silences human rights defenders.

Recommendations:

- ➔ Clarify that stakeholder engagement is a necessary (non-optional) element of any HREDD process, and align minimum requirements for engagement with the UNGPs, including stakeholder access to information and protection for participants.
- ➔ Human rights defenders, other vulnerable groups, and technical experts should be explicitly included as key stakeholder groups, given the relevance of their experience and knowledge to understanding the rights impacts of the tech sector.



Complaints procedure

The Directive includes in Article 9 the welcome requirement that companies allow for persons and organisations to submit complaints directly to them in case of legitimate concerns regarding adverse human rights and environmental impacts. This “complaints mechanism” has the potential to improve access to corporate decision-makers for rightsholders, bolster transparency, and increase engagement between tech companies and those most affected by their work.

Nevertheless, as currently drafted, this mechanism is only available to persons who are already or are likely to be affected, trade unions and worker representatives as well as CSOs active in areas related to the value chain. The Directive could be strengthened by clarifying the mechanism will be available to a broad range of actors, including digital rights experts and human rights defenders broadly involved in and impacted by the sector and its value chains. Further, the lack of required remediation elements in the mechanism outlined in Article 9 limits its ability to ensure firms are held accountable for violations to rightsholders themselves.

Recommendations:

- ➔ Amend the conception of the complaints procedure included in the Directive by clarifying that a wide range of stakeholders will be able to use it.
- ➔ Consider expanding the scope and purpose of the complaints procedure to include remediation of grievances, in line with the UNGP remediation requirements.



Liability

The Directive provides for consequences in the form of administrative sanctions, penalties and civil liability for failure to adhere to its requirements and for not addressing impacts on human rights and the environment, and for resulting harm. This constitutes the “teeth” of the Directive and, for the tech sector, represents an opportune effort to bolster corporate accountability and change the calculus of risk in tech company boardrooms where human rights implications are currently too rarely considered.

There are at least two areas in which the Directive's approach to liability can be strengthened.

First, a broad range of exceptions or mitigating circumstances to liability are available to companies under Articles 20 and 22, which would allow reckless tech companies to sidestep their responsibilities. For instance, as currently drafted, companies will not be liable for damages caused by an adverse impact arising from the activities of an indirect partner with whom it has an “established business relationship”, so long as the company has taken contractual (and third-party) verification measures to cascade ‘compliance’ in its value chain (and had reason to expect this was adequate). For tech companies, which have constantly changing impacts, this could function as a way to avoid consequences through superficial inclusion of contractual clauses and third-party verification, leaving harmed individuals and groups without redress.

Second, impacted individuals, civil society organisations and HRDs have long struggled to access sufficient information to hold tech companies accountable for harm. The costs associated with this access have been prohibitive, and particularly so where rightsholders are tasked with proving irresponsible corporate behaviour. The Directive is currently silent on addressing either of these obstacles. It should explicitly insist on access to information to allow informed stakeholder engagement, and for those harmed to gather evidence of poor company performance.

Recommendations:

- ➔ Revise provisions relating to liability limitations to ensure companies fulfil their obligations under the Directive and are not able to use contractual clauses or third party verification as shields against liability for inadequate due diligence.
- ➔ Provide for access to information by rightsholders in pursuing corporate liability, and reverse the burden of proof in such circumstances so companies are required to prove they have met the requirements of the law and taken all necessary steps to prevent harm, instead of requiring the party which brings to light infractions to first bring information that is extremely hard or impossible for them to access.



Conclusion

The Directive is a pioneering step towards ensuring people and their rights are placed at the centre of the tech industry. Ultimately, the Directive should ensure the stipulations provided by the UNGPs are reflected in this legislation as the minimum standard against which companies must comply. Further, on adoption of the Directive, it will be critical that guidelines for the tech sector, and more specifically the surveillance industry, are developed through consultation with all stakeholders, including digital and human rights groups, as envisioned by Article 13.

The Commission's proposed Directive will be subject to amendments and approval by the European Parliament and governments over the coming months. This will provide an opportunity for the European Commission, Parliament and Council to continue to receive sector-specific inputs, particularly from [digital rights experts](#), human rights groups and defenders, and individuals who have first-hand experience of the sector's negative impacts, to inspire changes that will strengthen the Directive. Incorporating changes suggested as a result of these consultations will ensure it is fit for purpose and a model for other jurisdictions, ushering in the long-awaited start of true corporate accountability in the technology sector.



**Business & Human Rights
Resource Centre**

Business & Human Rights Resource Centre is an international NGO which tracks the human rights impacts of over 10,000 companies in over 180 countries, making information available on our 10-language website.

AUTHOR:

Gayatri Khandhadai, Business & Human Rights Resource Centre

With thanks to the Business & Human Rights Resource Centre team for their support and contributions.