**20 May 2022**

# Privacy International's submission to the European Commission consultation on the proposal for a directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937

## Introduction

Privacy International ("PI")[1] welcomes the opportunity to provide feedback on the European Commission's proposal for a directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence (the "Directive").

PI is a London-based non-profit, non-governmental human rights organisation (Charity Number: 1147471) founded in 1990 that advocates globally against government and corporate abuses of data and technology, and overreaching state and corporate surveillance. It researches, exposes and litigates harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. Within its range of activities, PI investigates how people's personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Commission and Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights and the UN Refugee Agency.

We strongly support the Commission's initiative to introduce EU-wide mandatory due diligence that encompasses companies' entire value chain. We are however concerned that many of the human rights abuses we encounter and fight in our work may not be identified and/or remedied by the obligations established in the Directive. The technology and surveillance industry has ushered in an entirely new sphere of actual and potential human rights abuses, defying traditional detection, enforcement and remedy mechanisms, and leaving legal frameworks to play constant catch-up. There is growing recognition[2] that technology companies have so far evaded scrutiny of their human rights impacts, due to a number of factors such as the complexity of their products, services and activities, the opacity with which they frequently operate, and the variety of human rights impacts they can be responsible for. This is why, for example, the Office of the United Nations High Commissioner for Human Rights ("OHCHR") has set up an initiative to provide authoritative guidance on the application of the United Nations Guiding Principles ("UNGPs") to the activities of technology companies – the B-Tech project.[3]

This Directive is a unique opportunity to reassert companies' responsibility to respect human rights as set out in the UNGPs, and to create an EU-led global standard for corporate human rights

[1] PI is an international non-governmental organisation that campaigns against companies and governments who exploit individuals' data and technologies. PI employs specialists in their fields, including technologists and lawyers, to understand the impact of existing and emerging technology upon data exploitation and our right to privacy, https://privacyinternational.org/.
[2] Business & Human Rights Resource Centre, Human rights due diligence within the tech sector: Developments and challenges (Opinion) (1 December 2020), https://www.business-humanrights.org/en/blog/human-rights-due-diligence-within-the-tech-sector-developments-and-challenges/.
[3] OHCHR, B-Tech Project, https://www.ohchr.org/en/business-and-human-rights/b-tech-project.

accountability. We would therefore hope that most activities of technology companies fall squarely within scope of the Directive. In this submission we will detail our concerns with the current text, supported by some examples from our work, and provide recommendations for improvement.

## Summary of concerns

PI's main concern with the current draft of the Directive has to do with its scope – both "personal" (which companies it will apply to, as defined in Article 2) and "material" (which sectors and human rights and environmental adverse impacts it covers, as defined in Articles 2(1)(b) and 3(c) and (l)). The current scope of the Directive is such that many of the most problematic companies in the technology and surveillance industry will not be subject to these obligations, and many potential or actual human rights abuses they perpetrate will therefore evade identification and remediation.

With regards to personal scope, defined in Article 2, the draft states that "small and medium sized enterprises (SMEs) that include micro companies and overall account for around 99% of all companies in the Union, are excluded from the due diligence duty". This is a staggering number, raising questions as to the purpose of this legislation and the impact it will have. Due diligence is now a common corporate practice for both large and small enterprises, and UNGP 15 requires that all companies have in place "policies and processes appropriate to their size and circumstances, including [...] A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights". It is therefore unclear why it was considered disproportionate to extend application of the Directive to a larger number of companies – both for companies established in the Union and those established in a third country.

Moreover, Article 1(1)(a) limits companies' due diligence duty regarding value chain operations to those carried out by "entities with whom the company has an *established* business relationship" [emphasis added]. Again, the rationale for this limitation is unclear – a number of human rights abuses can be perpetrated or encouraged through a single, one-off, time-limited business relationship.

With regards to material scope, the Article 2(1)(b) shortlist of "high-impact sectors" that will raise a due diligence duty if a company falls below the employee and/or turnover thresholds of Article 2(1)(a) seems arbitrary and inconsiderate of the numerous, complex and varied ways in which human rights adverse impacts can arise. The decision to align the list with guidance from the OECD is not explained – and the lack of OECD sector-specific guidance in a sector is no indication of that sector's potential to perpetrate human rights abuses. It also seems to contradict the intention for the Directive to set up a horizontal framework.

Finally, as to the list of human rights and international conventions in the Annex to the Directive, it's unclear to us why only certain rights were selected from the international conventions as in scope of the Directive. For example, the following rights are effectively excluded from scope of the Directive, while being rights that can easily be (and often are) violated by companies (this is a non-exhaustive list):

- Article 1(1) of the ICCPR – peoples' right of self-determination (to freely pursue their economic, social and cultural development)
- Articles 2 and 3 of the ICCPR, and Article 21 of the EU Charter of Fundamental Rights – the right to non-discrimination on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status
- Article 19 of the ICCPR, Article 19 of the UDHR and Article 11 of the EU Charter of Fundamental Rights – the right to hold opinions without interference and the right to freedom of expression

Companies are required to abide by all rights within international conventions – all such rights should therefore be subject to the due diligence duty. Notably, UNGP 12 provides that "Because

business enterprises can have an impact on virtually the entire spectrum of internationally recognized human rights, their responsibility to respect applies to all such rights. In practice, some human rights may be at greater risk than others in particular industries or contexts, and therefore will be the focus of heightened attention. However, situations may change, so all human rights should be the subject of periodic review."

These are particular concerns in the technology and surveillance sector, where companies that are new, small, and/or with little resources or employees can create, perpetrate or enable profound threats to many different human rights. The nature of technology products and services is such that one single "innovation" can have disproportionate adverse impacts on a number of people. This can notably happen through the one-off provision of a product or service to a government. **We set out below a few examples identified in PI's work, to show that the potential and actual adverse impacts caused by these companies or industries would not be subject to the Directive's due diligence duty in its current shape**.

# Examples

## Data analytics – The example of Palantir

The data analytics industry provides analytical techniques to search, aggregate, and cross-reference large data sets in order to develop intelligence and insights, and thereby inform private or public decision-making. While the value proposition of data analytics does not in itself necessarily raise human rights risks, data analytics companies can give rise to human rights risks through the clients they provide their services to, and/or through the process used to provide these. Data analytics have the potential to discriminate and harm people in multiple ways. For example, they can be used to identify aberrant data amongst larger sets, to facilitate discrimination against specific groups and activities. Or they can be used to draw conclusions about large groups of people in order to make decisions about them or make public policies, while some people will be excluded from consideration because their data is not included in the sets, or the quality of their data is poorer.[4]

PI has worked in the past few years to challenge the global spread (without adequate safeguards and human rights due diligence) of data analytics in government, law enforcement and national security, fueled by contracts and partnerships with companies such as Palantir Technologies ("Palantir"). Palantir is a company based in the US, founded in 2003, that sells data integration and analytics platforms, often to national security, defence and law enforcement agencies, and other government departments. Palantir's CEO, Alex Karp, has previously acknowledged that its product is used to target and kill terrorists[5] - during the company's Q4 2020 earnings call, its Chief Operating Officer Shyam Sankar declared their intention as having Palantir "inside of every missile, inside of every drone".[6] The company has also been closely involved with US Immigration and Customs Enforcement (ICE), and has been considered in part responsible for the detainment and deportation of undocumented migrants and separation of immigrant children from their families.[7] Palantir has also been reported to have secretly used New Orleans to test its predictive policing technology,[8] a technology now widely known to fuel discrimination, exclusion and various human

[4] PI, Big Data (8 February 2018), https://privacyinternational.org/explainer/1310/big-data.
[5] Isobel Asher Hamilton, 'Our product is used on occasion to kill people': Palantir's CEO claims its tech is used to target and kill terrorists (26 May 2020), Business Insider, https://www.businessinsider.com/palantir-ceo-alex-karp-claims-the-companys-tech-is-used-to-target-and-kill-terrorists-2020-5?op=1&r=US&IR=T.
[6] Motley Fool Transcribing, Palantir Technologies Inc. (PLTR) Q4 2020 Earnings Call Transcript (16 February 2021), https://www.fool.com/earnings/call-transcripts/2021/02/16/palantir-technologies-inc-pltr-q4-2020-earnings-ca/.
[7] Edward Ongweso Jr, Palantir's CEO Finally Admits to Helping ICE Deport Undocumented Immigrants (24 January 2020), Vice, https://www.vice.com/en/article/pkeg99/palantirs-ceo-finally-admits-to-helping-ice-deport-undocumented-immigrants.
[8] Ali Winston, Palantir has secretly been using New Orleans to test its predictive policing technology (27 February 2018), The Verge, https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.

rights abuses.[9] We are aware that this technology has been used in various EU countries, including Denmark and Germany, as well as by the European police agency Europol.[10]

It is common practice for Palantir to offer its services to governments, including EU governments, at zero or very low cost. These contracts are often struck in the absence of public bids or other procurement processes, and converted into paying contracts after a 6-month or 1-year trial.[11] If Palantir regularly enters into zero-cost or low-cost contracts with EU governments, it is unclear whether the contribution of these business relationships to its annual turnover would exceed the threshold that would subject it to the Directive's due diligence duty. They are also unlikely to qualify as "established" business relationships, as currently defined in Article 3(f), at least for the initial trial or low-cost period. And yet even during a limited time period, the impact of Palantir's services on the activities of governments and other business partners can be profound, and once established, extremely difficult to scrutinize – decision-making through the use of companies' proprietary algorithms is by definition opaque and difficult to challenge. **We are therefore concerned that a third-country company like Palantir can have severe adverse impact on human rights in the EU and yet not be subject to the Directive's due diligence duty**.

## Online surveillance and facial recognition – The example of Clearview AI

Facial recognition is now a well-known technology that has raised alarm with many human rights independent experts and advocates around the world. Beyond constituting a serious interference with individuals' privacy, it is also known to cast a "chilling effect" on the exercise of other fundamental rights, such as the right to freedom of expression and the right to peaceful assembly.[12]

Another worrying practice increasingly developed and adopted by all kinds of public and private actors is known as Social Media Intelligence ("SOCMINT"), or more widely "Online Surveillance". Online Surveillance enables the monitoring and scraping of content posted by and about individuals online, and the subsequent analysis of this information to make decisions about them.[13] Despite the public availability of this information (which can be contested, as privacy settings are notoriously difficult to get right so that the information one wants to remain within private online circles actually is and remains so[14]), a stark divide between the public and the private spheres bears little relevance to modern societies where major parts of our economic, social and democratic lives are led online. It is misunderstanding the Internet to see it as a homogeneous, entirely public and fully accessible forum on which everyone consents to their personal information being "fair game" for all to grab as soon as it has entered a technically public part of the Internet.

The UN High Commissioner for Human Rights states in their report on the right to privacy in the digital age that "[t]he protection of the right to privacy is not limited to private, secluded spaces, such as the home of a person, but extends to public spaces and information that is publicly available (see CCPR/C/COL/CO/7, para. 32). For example, the right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station, thereby

[9] Tim Lau, Predictive Policing Explained (1 April 2020), Brennan Center for Justice, https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
[10] PI and No Tech for Tyrants, All roads lead to Palantir (September 2020), https://privacyinternational.org/sites/default/files/2021-11/All%20roads%20lead%20to%20Palantir%20with%20Palantir%20response%20v3.pdf. See also Arthur Neslen, Pushback against AI policing in Europe heats up over racism fears (20 October 2021), Reuters, https://www.reuters.com/article/europe-tech-police-idINL8N2R92HQ.
[11] Daniel Howden, Apostolis Fotiadis, Ludek Stavinoha and Ben Holst, Seeing stones: pandemic reveals Palantir's troubling reach in Europe (2 April 2021), The Guardian, https://www.theguardian.com/world/2021/apr/02/seeing-stones-pandemic-reveals-palantirs-troubling-reach-in-europe.
[12] PI, Facial Recognition, https://privacyinternational.org/learn/facial-recognition.
[13] PI, Social Media Intelligence – Explainer (23 October 2017), https://privacyinternational.org/explainer/55/social-media-intelligence.
[14] PI, Most cookie banners are annoying and deceptive. This is not consent. (21 May 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. PI, Facebook - Profile Settings (7 January 2021), https://privacyinternational.org/guide-step/3959/facebook-profile-settings.

observing individuals. Similarly, when information that is publicly available about an individual on social media is collected and analysed, it also implicates the right to privacy. The public sharing of information does not render its substance unprotected." [15] Similarly, the UN Human Rights Committee has urged caution with regard to this form of surveillance: "The mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated. [...] The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent and transparent scrutiny and oversight must be exercised over the decision to collect the personal information and data of those engaged in peaceful assemblies and over its sharing or retention".[16]

One company has developed a technology that embodies the dystopian union of facial recognition and online surveillance – Clearview AI, Inc. ("Clearview"). Clearview is a company based in the US, founded in 2017. Their sole product (for now) is a searchable faceprint database, built by scraping the public Internet and collecting all photos of people's faces found online, and running them through their facial recognition algorithm. The current version of their database contains over 20 billion facial images.[17] They sell access to this database to law enforcement agencies in the US and other countries, and are understood to have previously sold their services to private individuals and companies as well.

Following legal complaints by PI and other NGOs, Clearview has been found by a number of regulators to have violated data protection and human rights laws through its indiscriminate, secret and non-consensual collection of people's faces – notably by data protection authorities in the UK, France and Italy.[18] Further decisions are awaited from the Greek and Austrian authorities. The use of Clearview's services by law enforcement agencies has also been found unlawful in a number of countries.[19] Most recently, the American Civil Liberties Union (ACLU) reached a settlement with Clearview after suing them for violation of Illinois privacy laws.[20] The suit had been brought by the ACLU alongside a group of organisations defending the rights of survivors of domestic violence and sexual assault, undocumented immigrants, communities of color, and members of other vulnerable communities. The company is now banned across the US from making its faceprint database available to most businesses and other private entities, and must cease selling access to its database to any entity in Illinois (including law enforcement) for five years.

Clearview's business model, which relies on the indiscriminate collection and biometric processing of people's faces, represents a profound threat to the safety and exercise and protection of human rights of individuals whose photos are scraped – who include a considerable number of EU citizens and residents. Yet **as the current draft of the Directive stands, Clearview would not be required to perform any due diligence on its operations and business relationships – as a "third-country company", it does not generate sufficient turnover in the EU to be subject to the duty**. It also does not operate in any of the sectors considered "high-impact" under Article 2(1)(b) of the Directive. Finally, the often fleeting nature of its relationships with governments and law

[15] United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/39/29 (3 August 2018), https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commissioner-human.
[16] General Comment No. 37 on Article 21 of the International Covenant on Civil and Political Rights (Right of peaceful assembly), adopted by the UN Human Rights Committee, https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx.
[17] Clearview AI, Clearview AI Releases 2.0 Version of Industry Leading Facial Recognition Platform for Law Enforcement (25 March 2022), https://www.clearview.ai/clearview-ai-releases-2-version-of-industry-leading-facial-recognition-platform-for-law-enforce.
[18] PI, Challenge against Clearview AI in Europe, https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe.
[19] EDPB, Swedish DPA: Police unlawfully used facial recognition app (12 February 2021), https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en. Politico Pro, Belgian police watchdog rules use of Clearview AI 'unlawful' (3 October 2022), https://subscriber.politicopro.com/article/2022/03/belgian-police-watchdog-rules-use-of-clearview-ai-unlawful-00016045.
[20] American Civil Liberties Union, In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law (9 May 2022), https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois.

enforcement agencies (often providing free trials or one-off access) means that these wouldn't be considered "established business relationships" requiring it to exercise due diligence on these clients.

## AdTech

The AdTech (short for "advertisement technology") industry is made up of companies providing tools and services that connect advertisers with target audiences and publishers – such as data brokers, advertisers, apps and platforms.[21] These companies have created a complex ecosystem where individuals' data is treated as a commodity, collected from websites and digital services on which people rely for vital daily activities – without providing users any control over how their data is shared and repurposed. Companies in the industry then share this data with each other to create finely grained profiles of individuals, which are then used to target people with advertising (commercial and political), and feed into decisions that may affect human rights, such as voting, access to credit, employment, insurance or welfare benefits.

Targeted advertising can be discriminatory, manipulative, and exploitative.[22] For example, PI's research has shown that popular websites providing advice and support about mental health share user data with advertisers, data brokers and large tech companies,[23] while some menstruation apps share data with Facebook and other third parties.[24]

Many actors in the industry have faced and are still facing investigations by Data Protection Authorities, complaints and lawsuits globally.[25] A recent joint decision of EU data protection authorities, led by their Belgian counterpart, found that the AdTech industry's trade body "IAB Europe" had committed multiple violations of the EU GDPR in its processing of personal data in the context of its "Transparency and Consent Framework" (TCF) and the Real-Time Bidding (RTB) system.[26] This significant decision has effectively found that the consent mechanism present on 80% of the European internet had "deprived hundreds of millions of Europeans of their fundamental rights".[27]

Years of this industry's non-compliance with data protection legislation and disregard for the profound impact it can have on people's privacy, freedom of expression and to hold opinions have led to advertising supply chains being riddled with unlawfully collected data. Issues in the advertising supply chain are similar to traditional supply chain problems, for example in the clothing industry, such as issues with traceability. Companies in this industry should therefore be subject to the same due diligence obligations as others.

**But the nature of companies that make up the AdTech industry is such that their number of employees, turnover, and sector of activity would in most cases not make them subject to the**

[21] PI, AdTech, https://privacyinternational.org/learn/adtech.
[22] Norwegian Consumer Council, Out of Control – How consumers are exploited by the online advertising industry (14 January 2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.
[23] PI, Your mental health for sale – How websites about depression share data with advertisers and leak depression test results (September 2019), https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf.
[24] PI, No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data (9 September 2019), https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data.
[25] PI has complained about seven AdTech companies to data protection authorities in France, Ireland and the UK. See PI, Our complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad (8 November 2018), https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.
[26] Autorité de protection des données (Litigation Chamber), Decision on the merits 21/2022, Case number DOS-2019-01377, Concerning : Complaint relating to Transparency & Consent Framework (2 February 2022), available at https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf.
[27] ICCL, GDPR enforcer rules that IAB Europe's consent popups are unlawful (2 February 2022), https://www.iccl.ie/news/gdpr-enforcer-rules-that-iab-europes-consent-popups-are-unlawful/.

**Directive's due diligence duty**. This is highly concerning considering the complexity and extent of human rights adverse impacts they can perpetrate or assist their clients and suppliers in perpetrating.

### Electronics sector

The global generation of electrical and electronic waste (e-waste) is growing exponentially. Every year, more and more consumers buy new devices, or replace their malfunctioning, broken or out-of-date phones, computers, TVs and other electronics, generating e-waste at a huge scale - an increase of 2.5 million metric tons (Mt) on average every year globally.

Around the world, people generated some 53 million tons of e-waste in 2019, projected to grow to a staggering 74.7 million tons by 2030.[28] Recycling cannot keep up, even where infrastructures are developed: only 17.4% of 2019's global e-waste was collected and recycled formally. In fact, much of e-waste is exported illegally from high income to lower income countries, or is mixed up with other waste. It ends up improperly disposed of in landfills where toxins common in electronics like lead, mercury and cadmium can leach out and contaminate surrounding soils and groundwater.

Yet the current draft of the Directive only subjects companies of 250-499 employees in the textiles, agriculture and minerals extractions sectors (listed in Article 2(1)(b)) to the due diligence duty. This fundamentally ignores the growing problem of e-waste, whereby the link to environmental impacts is not made with the tech sector as it is with other sectors. One of the reasons why so many devices are produced, bought and thrown away every year is that software that runs on devices quickly goes out of date and becomes a security and privacy risk when it does so.[29] Tech companies have also been known to slow down older software, so that people were misled into believing they should replace their devices – thereby creating more unnecessary waste.[30]

**We are therefore concerned that many companies involved in the electronics supply chain will not be subject to the due diligence duty, so that the problem of e-waste will go largely ignored**.

## Recommendations

The examples above indicate that a number of loopholes in the current draft of the Directive will allow a considerable number of potential and actual human rights adverse impacts to go undetected. We therefore recommend that:

1. The Directive be made to apply to all **companies formed in accordance with the legislation of a Member State, regardless of their number of employees, net turnover or sector of activity**. To address the potential burden of compliance for SMEs (identified in the Directive's explanatory text on Proportionality), we would be in favour of establishing thresholds for the extent of due diligence that companies must perform, and providing extensive guidance and financial support to SMEs during the Directive's implementation stage.

2. The Directive be made to apply to all **companies formed in accordance with the legislation of a third country**, provided that their activity raises a reasonable likelihood of impact on one or more of the rights of individuals in the EU protected by the international conventions listed in the Annex, Part I Section 2.

---

[28] Vanessa Forti and others, The Global E-waste Monitor 2020, https://www.itu.int/en/ITU-D/Environment/Documents/Toolbox/GEM_2020_def.pdf.
[29] PI, Best Before date policy brief: Device sustainability through long-term software support (29 October 2021), https://privacyinternational.org/advocacy/4636/best-date-policy-brief-device-sustainability-through-long-term-software-support.
[30] See for example BBC, Apple fined for slowing down old iPhones (7 February 2020), https://www.bbc.co.uk/news/technology-51413724.

3. The Directive be made to apply to the value chain operations carried out by entities with whom the companies have **any business relationship**, not only established relationships.

4. **The condition in Article 2(1)(b) and 2(2)(b) that 50% of a company's turnover was generated in one of more of the listed sectors be deleted**. All sectors of activity can give rise to human rights adverse impacts – the Directive's current emphasis on specific sectors for companies that fall below a certain employee and turnover threshold risks detracting attention from other sectors that can cause such impacts in a less easily identifiable way, as well as providing them with a justification for their lack of due diligence.

5. **All rights enshrined in the international conventions listed in Section 2 of Part I of the Annex to the Directive be in scope of the Directive**. Section 1 of Part I of the Annex to the Directive (list of rights) should be deleted, and only Section 2 (list of international conventions) should be preserved.