23 February 2022

Privacy International's submission to the UN High Commissioner for Human Rights' report on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies

Introduction

Privacy International (PI)[1] welcomes the opportunity to provide input to the forthcoming report by the UN High Commissioner for Human Rights (HCHR) on the practical application of the United Nations Guiding Principles on Business and Human Rights (UNGPs) to the activities of technology companies to be presented at the 50th session of the Human Rights Council in June 2022.[2]

The technology industry has ushered in an entirely new sphere of potential human rights abuses, defying traditional detection, enforcement and remedy mechanisms, and leaving legal frameworks to play constant catch-up. This report is a significant opportunity to reassert the relevance of the UNGPs to the activities of technology companies and their relations with states, to help state and non-state actors identify, assess and remedy tech-enabled human rights abuses.

PI will address the four set themes of the consultation in turn, providing relevant examples of abuse it has identified in its research work around the world, and recommendations as to how these can be addressed to uphold application of the UNGPs. The focus of our submission will be on situations where technology companies are contracted or otherwise used by states to deliver public services, although we will in some places address the activities of technology companies where no relation with the state exists. PI has recently published a set of safeguards to address issues common to public-private partnerships that involve surveillance technology and/or the mass processing of data, which are relevant to this consultation.[3]

In summary, PI recommends the HCHR report:

- highlights the systemic lack of accountability of this industry, national authorities' slow or non-existent enforcement of privacy laws against its exploitative practices, and its relations with governments;
- reasserts the need for states to implement strong safeguards against abuses of surveillance technology;
- asserts the need for transparency over the use of data analytics in public sector decision-making, and calls for strict safeguards around their use;

---

[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] OHCHR, Call for input to the High Commissioner report on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies, https://www.ohchr.org/EN/Issues/Business/Pages/CFI-ungps-tech-companies.aspx.

[3] PI, Safeguards for Public-Private Surveillance Partnerships, December 2021, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf.

- calls for public authorities to conduct individual human rights risk and impact assessments (HRIAs) as well as data protection impact assessments (DPIAs) during any surveillance technology procurement process, in addition to companies conducting Human Rights Due Diligence (HRDD) on any prospective state client's end-use of their technology;
- asserts that public authorities should not systematically use surveillance and data processing systems deployed for private purposes and/or data derived from these systems;
- reasserts the obligation to consider legality, necessity and proportionality every time a technology is proposed for use by public authorities;
- asserts the need for tech companies to provide transparency over their technologies and to make their algorithms auditable, and for states to mandate such transparency when these technologies are used to deliver public functions;
- recommends that a use policy is developed to govern a public authority's use of a particular technology;
- reasserts that contracts between public authorities and tech companies must point to redress mechanisms for complaints handling and enforcement of sanctions for abuses or violations of human rights;
- asserts the need for courts to always remain accessible despite the existence of independent regulators;
- reaffirms that outsourcing of surveillance powers to private companies does not absolve states of their human rights obligations.

1. Addressing human rights risks in business models

The B-Tech project has defined the term "business model" to denote "the value a company seeks to deliver, and to whom and how it delivers that value in the pursuit of commercial success".[4] In that sense, issues with tech companies' business models can arise (1) from the nature of the product/service they provide, (2) the clients they provide these to, and/or (3) the process through which they provide these.

PI would like to draw the HCHR's attention to a number of technology industries whose business models are predicated on perpetrating certain abuses of human rights, and whose very existence thereby perpetrates or helps perpetrate those abuses, or are highly likely to encourage or facilitate such abuses.

AdTech (advertisement technology)

The term AdTech designates tools and services that connect advertisers with target audiences and publishers. The AdTech industry has created an 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, such as data brokers, advertisers, apps and platforms 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 access to credit, insurance or welfare benefits.

Targeted advertising can be discriminatory, manipulative, and exploitative.[5] For example, PI's research has shown that popular websites providing advice and support about mental health

[4] UN High Commissioner for Human Rights, B-Tech Foundational Paper, Addressing Business Model Related Human Rights Risks, https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf.
[5] 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.

share user data with advertisers, data brokers and large tech companies, [6] while some menstruation apps share data with Facebook and other third parties.[7]

PI is therefore concerned that companies involved in the AdTech ecosystem rely on a Value Chain[8] (as defined in the B-Tech Foundational Paper on Addressing Business Model Related Human Rights Risks) that (1) is opaque, (2) has been alleged to breach various countries' privacy laws[9], and (3) facilitates hate, disinformation and whittling of democratic processes.[10] While civil society actors have raised the alarm about these companies for years, these concerns remain largely unanswered and the industry keeps flourishing, exploiting billions of individuals' data every day. We are particularly concerned that the industry is now also selling data to government agencies, law enforcement and intelligence agencies in various countries, often bypassing legal requirements for obtaining such data.[11]

PI recommends that the HCHR report highlights the systemic lack of accountability of this industry, national authorities' slow or non-existent enforcement of privacy laws against its exploitative practices, and its relations with governments.

Spyware/Surveillance Technology

Companies in the surveillance technology industry sell a wide range of systems used to identify, track and monitor individuals and their communications – for governments' spying and policing purposes. Their entire business model (from Value Proposition to Value Chain) relies on, and facilitates, a number of human rights abuses by governments worldwide.

As PI has repeatedly affirmed, spyware permitting hacking capabilities can present unique and grave threats to our privacy and security. Even where governments conduct surveillance in connection with legitimate aims, such as gathering evidence in a criminal investigation or intelligence, they may never be able to demonstrate that hacking as a form of surveillance is compatible with international human rights law. To date, however, there has been insufficient public debate about the scope and nature of these powers and their privacy and security implications.

In August 2021, UN human rights experts called on all states to impose a global moratorium on the sale and transfer of surveillance technology until they have put in place robust regulations that

---

[6] 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.

[7] 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.

[8] As defined in the B-Tech Foundational Paper on Addressing Business Model Related Human Rights Risks, https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf.

[9] 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. See also Irish Council for Civil Liberties, Lawsuit against online advertising industry, 15 June 2021, https://www.iccl.ie/news/press-announcement-rtb-lawsuit/.

[10] PI has complained to the UK data protection authority against the CT group of companies, which provides data analytics services for political campaigning purposes, raising concerns about the impact that such services can have on free democratic elections and about the ability of individuals to exercise their data rights in the process. See PI, Challenge to Hidden Data Ecosystem in Political Campaigning, https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem-political-campaigning.

[11] See PI, Benefitting whom? An overview of companies profiting from "digital welfare", 25 November 2020, https://privacyinternational.org/long-read/4144/benefitting-whom-overview-companies-profiting-digital-welfare; PI, Shedding light on the DWP Part 1 - We read the UK welfare agency's 995-page guide on conducting surveillance and here are the scariest bits, 14 February 2021, https://privacyinternational.org/long-read/4395/shedding-light-dwp-part-1-we-read-uk-welfare-agencys-995-page-guide-conducting; Center for Democracy & Technology, Report – Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers, 9 December 2021, https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/.

guarantee its use in compliance with international human rights standards.[12] Since 2018, civil society organisations have been making damning revelations about the widespread abuses of NSO Group's spyware by various governments around the world.[13] As PI's report, together with Amnesty International and the Centre for Research on Multinational Corporations (SOMO)[14] has shown, the lack of transparency around NSO Group's corporate structure and the lack of information about the relevant jurisdictions within which it operates are significant barriers in seeking prevention of, and accountability for, human rights violations reportedly linked to NSO Group's products and services.[15] This is just one example of how the surveillance technology industry has been allowed to proliferate with little challenge, and of how the calls for safeguards by civil society and by the UN experts have been largely ignored.

PI has developed safeguards for the compliance of government hacking with international human rights law,[16] and recommends their application to the use of spyware products.

PI recommends that the HCHR report reasserts the need for states to implement strong safeguards against abuses of surveillance technology.

Data analytics

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, the data analytics industry 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. First, they can be used to identify aberrant data amongst larger sets, to facilitate discrimination against specific groups and activities.[17] Second, data analytics is used to draw conclusions about large groups of people, while some will be excluded because their data is not included in the sets, or the quality of their data is poorer, thereby excluding them from consideration when devising public policies.[18]

PI has worked in the past few years to challenge the global spread of data analytics practices, by companies such as Palantir, whose tools may pose a real danger to people in vulnerable positions such as at international border crossings.[19] More recently, PI shed light on its contracts with the national health service (NHS) and other critical government departments in the UK.[20] We faced a complete lack of transparency and accountability with regards to the role of Palantir's data analytics in the formulation of public policy – leaving us and the public unable to understand its rationale, nor to challenge any potential underlying human rights abuses.

---

[12] Press release, Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech, 12 August 2021, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E. See also Report of the UN Special Rapporteur on freedom of opinion and expression, A/HRC/41/35, 28 May 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736.

[13] Amnesty International, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, 19 July 2021, https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/.

[14] Amnesty International, PI and SOMO, Operating from the Shadows: Inside NSO Group's Corporate Structure, June 2021, https://www.privacyinternational.org/report/4531/operating-shadows-inside-nso-groups-corporate-structure.

[15] The New York Times, Hacking a Prince, an Emir and a Journalist to Impress a Client, 31 August 2018, https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html.

[16] PI, Government Hacking and Surveillance: 10 Necessary Safeguards, https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf.

[17] Latanya Sweeney, Discrimination in Online Ad Delivery, Data Privacy Lab, 28 January 2013, https://dataprivacylab.org/projects/onlineads/1071-1.pdf.

[18] PI, Big Data, 8 February 2018, https://privacyinternational.org/explainer/1310/big-data.

[19] PI, Who supplies the data, analysis, and tech infrastructure to US immigration authorities?, 9 August 2018, https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities.

[20] PI and No Tech for Tyrants, All Roads Lead to Palantir, 29 October 2020, https://privacyinternational.org/report/4271/all-roads-lead-palantir.

PI recommends that the HCHR report asserts the need for transparency over the use of data analytics in public sector decision-making, and calls for strict safeguards around their use to avoid discrimination, entrenchment of inequalities and injustice, and lack of public accountability.

2. Human Rights Due Diligence and end-use

While PI's comments in this section will remain limited to the application of HRDD requirements to end-use, as set by the consultation themes, we consider that these requirements ought to apply to the entirety of a technology company's product/service lifecycle in addition to end-use – from business model development, to product/service design, to marketing practices, to product/service sale and delivery, to provision of support services, to post-contract assessments. We note that the 2021 Human Rights Council resolution on the right to privacy in the digital age recognised the importance of applying HRDD to the whole life cycle of a technology, confirming the recommendation contained in the OHCHR report on right to privacy and Artificial Intelligence.[21]

Responsibility for the conduct of Human Rights Due Diligence

HRDD on end-use of tech products/services by states or authorities involves two essential aspects: (1) tech companies ought to perform HRDD when they decide whether to sell their products/services to a certain state/authority for a certain end-use (as required by UNGPs 15 and 17), and (2) states or authorities ought to conduct appropriate assessments of the human rights impact of deploying a certain technology or system on human rights. PI's research on public-private partnerships has shown that states or authorities often ignore aspect (2), instead assuming that the responsibility to consider human rights risks falls with the company providing a product or service. For example, when the municipality of Como in Italy performed a DPIA for the deployment of facial recognition technology supplied by company Huawei, the DPIA did not assess the impact of facial recognition on citizens' enjoyment of human rights, nor did it assess the accuracy of the algorithm provided. To our knowledge no separate HRIA was conducted.[22]

PI recommends that authorities conduct individual DPIAs and HRIAs during any surveillance technology procurement process, in addition to companies conducting HRDD on any prospective state client's end-use of their technology.

Use of privately deployed technologies for states' purposes

Another recurrent issue PI has observed is that of technologies deployed for private purposes being co-opted by public authorities for policing or other surveillance purposes, without following procurement processes nor applying safeguards. For example, we have previously seen Amazon Ring entering into agreements with police forces to grant them access to private surveillance networks in the United States of America,[23] or a retail surveillance network deployed by facial recognition company Facewatch offered for use by police forces in the UK.[24]

In order to comply with UNGPs 5 and 6, PI recommends that public authorities should not systematically use surveillance and data processing systems deployed in private spaces and/or data derived from these systems. Any use of such systems should be on an ad hoc, strict necessity basis following the relevant legal framework, and accompanied by the transparency and due process standards required of any public access to companies' data or procurement of their services.

---

[21] Resolution A/HRC/RES/48/4.
[22] PI, How facial recognition is spreading in Italy: the case of Como, 17 September 2020, https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como.
[23] PI, One Ring to watch them all, 25 June 2020, https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.
[24] PI, Cooperating with Who?! Answers Needed as UK Retailer Southern Co-Op Tests Facewatch, 9 December 2020, https://privacyinternational.org/advocacy/4342/cooperating-who-answers-needed-uk-retailer-southern-co-op-tests-facewatch.

Legality, Necessity and Proportionality of end-use

As part of meeting their HRDD obligations, states and tech companies ought to consider the legality, necessity, and proportionality of a technology's proposed end-use:

- Legality - When considering the need for, and the deployment of a technology to address a public need or fulfil a public function, states must consider whether an appropriate legal framework authorises the use of such technology, by specific authorities, for the specific purpose it is intended for (general legislation, such as one granting surveillance blanket powers, will not be sufficient).
- Necessity - a necessity assessment must be conducted to clearly demonstrate that recourse to a company's particular technology or data analytics system is necessary to achieve defined, legitimate goals, rather than a mere advantage.
- Proportionality - a proportionality assessment must be conducted to measure the adverse impact on individuals' human rights and demonstrate that it is justified by a corresponding positive impact on individuals' welfare. These assessments should take into account the potential chilling effects on other rights such as the rights to freedom of expression and freedom of assembly and association, which can be affected by surveillance and data processing systems in ways that can be difficult to anticipate and measure.

PI suggests that the HCHR report reasserts the need to apply the test of legality, necessity and proportionality every time a technology is proposed for use by public authorities.

3. Accountability and remedy

Transparency, a preliminary requirement

Accountability and the availability of remedy in relation to the activities of tech companies first require appropriate transparency. But transparency is notoriously difficult to obtain in such contexts – in our experience, tech companies systematically brandish their intellectual property rights and commercial interests as justifications to withhold any substantive information about their technologies, in particular any underlying algorithms. This was the case, for example, when PI obtained, through requests under the UK's Freedom of Information Act 2000, a contract between Amazon and the UK's National Health Service – which was heavily redacted for reasons of Amazon's commercial interest.[25] This is particularly problematic when these technologies are used by states to deliver their public functions, such as when algorithms are used to distribute welfare benefits.[26] Reliance on data-driven technologies has been shown to entrench inequalities and injustice, without providing individuals with the ability to question the decisions made by these technologies or by their users.

PI recommends that the HCHR report asserts the need for tech companies to provide transparency over their technologies and to make their algorithms auditable, and for states to mandate such transparency when these technologies are used to deliver public functions.[27]

Avoiding function creep

Function creep is a common issue in technology deployments – when technology deployed for one purpose is later used for a different purpose, without fresh new approval and oversight processes. For example, France attempted to use CCTV cameras during the Covid-19 pandemic to monitor mask wearing and social distancing in public spaces – the French data protection authority

[25] PI, Alexa, what is hidden behind your contract with the NHS?, 6 December 2019, https://privacyinternational.org/node/3298.
[26] PI, Shedding light on the DWP Part 2 - A Long Day's Journey Towards Transparency, 14 February 2021, https://privacyinternational.org/long-read/4397/shedding-light-dwp-part-2-long-days-journey-towards-transparency.
[27] For further detail on the concrete measures this requires, please see section I of PI's Safeguards for Public-Private Surveillance Partnerships, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf.

disapproved.[28] Function creep threatens to obfuscate the potential for a technology use to enable human rights abuses, as the public gets used to the presence of a technology and is thereby not prompted to question its further use.

PI urges the High Commissioner to highlight that once a technology is approved for use, a technology use policy be developed to govern the public authority's use of the technology, defining clear boundaries for the purpose and use of the technology, with an exhaustive list of authorized uses and a non-exhaustive list of prohibited uses – all based on what has been considered legal, necessary and proportionate. Any use of the technology that does not comply with this policy should undergo a new approval process. Also, an independent and effective oversight mechanism should be put in place.

Providing effective remedy

Tech companies should be required to assess any potential harm that can arise from the use of their products/services, and to design corresponding remedy mechanisms. Where tech companies are contracted by states to deliver public functions, things going wrong can lead to serious human rights abuses. Responsibility in such cases can even be difficult to assign between the technology provider (the company) and the technology user (the state). When a company's technology is used to perpetrate human rights abuses, the company's cooperation is essential to understand how rights were abused, who is responsible, and what redress is appropriate.

PI suggests that the report reasserts that contracts between states and tech companies point to redress mechanisms for complaints handling and enforcement of sanctions for abuses or violations of human rights – such as designating a relevant independent oversight body mandated with investigation and enforcement powers. Contracts should also require companies' full cooperation and transparency in case of an investigation.

Such oversight mechanisms should not exclude the victims' access to judicial remedies. Over the past few years, PI has faced and observed considerable weaknesses in the enforcement of privacy laws by regulators in various countries. More than three years after submitting complaints under the EU's General Data Protection Regulation (GDPR) against seven AdTech companies in France, the UK, and Ireland,[29] only one authority has fully investigated and taken enforcement action – two years after filing of our complaint.[30] While PI welcomes the establishment of regulators or oversight bodies to enforce data protection laws, we are concerned that states do not provide sufficient resources to enable them to fulfil their mandates. Their independence has also previously been questioned. [31] In addition, a decentralised, national-level enforcement mechanism has considerable limitations when dealing with global tech companies, who are able to pick favourable jurisdictions to establish their offices or designate data protection representatives. Due to these limitations, individuals seeking redress are neither obtaining proper access to nor quality of justice – complaints to regulators rarely provide the redress they are owed, nor do they provide binding precedents that would prevent further abuses by other actors.

PI recommends that the HCHR report asserts the need for courts to always remain accessible despite the existence of independent regulators – individuals should also be allowed to

[28] CNIL, La CNIL publie son avis sur le décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports, 12 March 2021, https://www.cnil.fr/fr/avis-sur-le-decret-video-intelligente-port-du-masque.
[29] 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.
[30] ICO, ICO takes enforcement action against Experian after data broking investigation, 27 October 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/.
[31] Digital Rights Ireland, DRI challenges independence of Ireland's Data Protection Authority, 28 January 2016, https://www.digitalrights.ie/dri-challenges-idependence-of-irelands-data-protection-commissioner/; European Commission, Data Protection: Commission sends a reasoned opinion to BELGIUM for lack of independence of its Data Protection Authority, 12 November 2021, https://ec.europa.eu/commission/presscorner/detail/en/inf_21_5342.

complain for breaches of privacy laws in the jurisdiction where they reside, instead of these complaints being taken to a place chosen by the company.

4. The state's duty to protect, or regulatory and policy responses

The state's duty under UNGP 1 to protect against human rights abuse includes a duty to take "appropriate steps to prevent, investigate, punish and redress" human rights abuse by third parties. This duty works alongside, and must keep in check, the corporate responsibility to respect human rights under UNGP 11. While states' *duty to protect* is understood as placing a heavier burden on states than the *responsibility to respect* places on companies, outsourcing surveillance or data processing capabilities to companies does not absolve the state of this "higher" duty to ensure human rights are not abused: "States should not relinquish their international human rights law obligations when they privatize the delivery of services that may impact upon the enjoyment of human rights".[32] In such cases, the state's responsibility even increases to ensure that it does not (1) itself perpetrate human rights abuses through the use of the company's technology, nor (2) cause or encourage the company to violate human rights.

The problem of states outsourcing surveillance became quite clear when PI researched the use by states and public authorities of the services of online surveillance and facial recognition company Clearview AI. This company, based in the US, has been found by various data protection authorities around the world to have breached privacy laws,[33] and is subject to a lawsuit in the US by the American Civil Liberties Union for violation of Illinois' biometrics privacy law.[34] But before these judicial and regulatory actions were launched, a number of public authorities around the world trialed or started using Clearview's services, seemingly disregarding the possibility that Clearview's product, or authorities' use of the product, could violate human rights. This demonstrates a systematic failure of states' oversight to ensure they meet their international human rights obligations when they contract with business enterprises to provide services that may have an impact on the enjoyment of human rights, contrary to UNGP 5.

PI suggests that the High Commissioner reaffirms that outsourcing of surveillance powers to private companies does not absolve states of their human rights obligations.

[32] UN Guiding Principles on Business and Human Rights, Commentary to UNGP 5, p.8.
[33] PI, All we want for Christmas is... Clearview AI to be banned (and looks like it's happening)!, 17 December 2021, https://privacyinternational.org/news-analysis/4721/all-we-want-christmas-clearview-ai-be-banned-and-looks-its-happening.
[34] ACLU, ACLU v. Clearview AI, https://www.aclu.org/cases/aclu-v-clearview-ai.