Response to the call for input for OHCHR report on the application of the UNGPs in the tech sector

These submissions are made by the members of the International Bar Association (IBA) Working Group on AI and Human Rights constituting of Maria Pia Sacco, Anurag Bana, Martijn Scheltema and Theodora Christou, with the support of IBA interns Sushant Khalkho and Yaroslava Mavlyutova.

CONTENTS

Theme 1: Addressing human rights risks in business models

A. Use of Artificial Intelligence in Business

1. Some business activities like gathering of large volumes of data, using 'algorithmic bosses' to mediate the relationship between workers and firms, using models that are informed by, or inform, the personal choices and behaviours of populations without their knowledge and consent, etc., may impose high human rights risk.[1] Thus, the impacts of digital technologies, particularly Artificial Intelligence ('AI'), on human rights requires immediate attention. Use of AI for law enforcement purposes raises right to privacy concerns in a criminal justice risk assessment since AI-based machines collect, store and analyse personal data of individuals. Even in healthcare diagnostics, vast quantities of sensitive data are collected for AI systems.

2. Furthermore, the right to freedom of opinion, expression, and information can be hindered. For instance, in the financial sphere wherein AI sets the credit ratings, an AI system may take certain opinions or communications with certain people into account while generating credit score, leading to a 'chilling effect'.[2] Credit rating algorithms, deployed to assess credit worthiness of natural persons, these may perpetuate and amplify patterns of inequality in labour and employment matters.[3] Since '*all* data' could be '*hiring* data', an individual may avoid communicating/associating with certain people, and not express their actual opinions or emotions[4] fearing the impact on their AI-generated employment profile.[5]

B. Solutions and Concluding Remarks

3. As noted in the B-Tech Project, technology companies, no matter what risks they may face, are obliged to initiate procedures to support human rights in the activities of their enterprises. Therefore, a business should initiate HRDD as early as possible, whenever a new activity or relationship occurs, given that human rights risks can be increased or mitigated at the stage of structuring contracts or other agreements.[6] Moreover, HRDD should be conducted on an ongoing

---

[1] Office of the UN High Commissioner for Human Rights, 'UN Human Rights Business and Human Rights in Technology Project (B-Tech)' (November 2019) p. 5 <https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Project_revised_scoping_final.pdf> accessed February 16, 2022 ('**B-Tech Scoping Paper**').

[2] Team AI Regulation, 'The Council of Europe's Recommendation for a Legal Framework on AI' (*ai-regulation.com*, 17 December 2021) <https://ai-regulation.com/council-of-europe-cahai-ai-recommendation/> accessed February 28, 2022.

[3] This is particularly true for 'Digital Welfare States'. The District Court of the Hague ordered the immediate halt of the Dutch government's risk indication system ('**SyRI**') whose aim was to predict the likelihood of a person committing benefit or tax fraud, or violating labour laws. The court criticised that the SyRI legislation demonstrated a 'serious lack of transparency' about how it worked. In the absence of more information, the system may, in targeting poor neighbourhoods, have led to discrimination on the basis of socioeconomic or migrant status. See Jon Henley, and Robert Booth, 'Welfare Surveillance System Violates Human Rights, Dutch Court Rules' (*The Guardian*, 5 February 2020) <https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules> accessed February 28, 2022.

[4] Mark Purdy, John Zealley, and Omaro Maseli, 'The Risks of Using AI to Interpret Human Emotions' (*Harvard Business Review*, 18 November 2019) <https://hbr.org/2019/11/the-risks-of-using-ai-to-interpret-human-emotions> accessed February 28, 2022.

[5] Filippo Raso et al, 'Artificial Intelligence & Human Rights: Opportunities & Risks' (Berkman Klein Center Research Publication No. 2018-6, 25 September 2018) pp. 29-31 <https://dash.harvard.edu/handle/1/38021439> accessed February 17, 2022.

[6] Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations* '*Protect, Respect and Remedy Framework*' (2011), principle 17

basis, since 'the human rights risks may change over time as the business enterprise's operations and operating context evolve'.[7] Finally, attempting to solve the problem of applying HRDD in the operation of machine learning AI, new evaluation techniques will need to be developed, such as human rights proxies. These will assist in the HRDD process.[8] The Council of Europe Ad Hoc Committee on Artificial Intelligence has worked on the development of policy guidelines on HRDD for AI and has developed human rights proxies as part of their HRDD assessment.[9]

Theme 2 - Human Rights Due Diligence and End-use

A. Preamble: End-use and HRDD

1. HRDD goes beyond a company's products and services, and includes all the value chain.[10] As the *B-Tech Scoping Paper* observes, software developers and producers of digital technologies (including AI) need to look, particularly at end users, 'as it is mostly in their use that human rights harms will manifest'. Moreover, companies are also expected to exercise leverage with their business partners and users, including through multi-stakeholder initiatives.[11]

B. AI, Risk to End Users and Human Rights Violations: Some Examples

2. The deployment of AI systems can have devastating consequences, in particular in the absence of a HRDD assessment. Opaqueness or lack of transparency in decision-making processes of AI systems poses serious challenges for end users to verify the accountability of the AI system. Bias and discrimination in AI decisions is another potential danger which when scaled up only further increases the negative effect. Early evidence suggests that aforementioned features of AI systems contribute to expansion, intensification or incentivisation of online and offline intrusions on the right to privacy and associated human rights (including the rights to health, social security, an adequate standard of living, work, freedom of assembly, freedom of expression and freedom of movement).[12]

3. Some examples include the utilisation of AI by law enforcement authorities which could result in violations of the right to liberty due to arbitrary arrests, or the freedom of assembly during demonstrations. The recent Chinese misuse of AI-enabled cyber surveillance technologies on ethnic minorities in Xinjiang province,[13] and Indian deployment of facial-recognition technology

---

<https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed February 16, 2022 ('**UNGPs**').

[7] UNGPs, principle 17(c).

[8] Council of Europe, 'Ad Hoc Committee on Artificial Intelligence (CAHAI) Policy Development Group (CAHAI-PDG)', CAHAI-PDG(2021)PV3 (Strasbourg, 27 May 2021) p. 5 <https://rm.coe.int/cahai-pdg-2021-pv3-abridged-meeting-report-5th-meeting-2763-0718-0035-/1680a2d8a1> accessed February 28, 2022.

[9] 'Possible Elements of a Legal Framework on Artificial Intelligence, Based on the Council of Europe's Standards on Human Rights, Democracy and the Rule of Law' (adopted by CAHAI on 3 December 2021) <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680a4e8a5> accessed February 23, 2022.

[10] UNGPs, principle 17.

[11] B-Tech Scoping Paper, p. 6.

[12] Office of the UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report* (15 September 2021, A/HRC/48/31) p. 1 <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx> accessed February 17, 2022.

[13] Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. To Profile a Minority' (*The New York Times*, 14 April 2019) <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> accessed February 17, 2022.

in law enforcement settings[14] are germane illustrations of the misuse of AI-enabled cyber surveillance technologies; Where AI has an advisory function, these risks may be more limited, compared with autonomous AI in which no humans are involved (eg, self-driving vehicles).[15] Although there is always a risk of overreliance by the human of the AI-generated advise.

4. Finally, AI systems do not exist in a vacuum and their impact on human rights may depend on the socio-economic contexts in which they operate, and on the nature of their end users.[16] This is particularly evident with, those products whose successful deployment is generally operated without the knowledge/consent of end users, such as for example, private surveillance products.[17] In addition to privacy concerns, repressive governments may employ AI to silence dissent, thus impacting freedom of association and expression.

C. Trade Measures for Export Control and Due Diligence Requirements

5. For a long time, the Wassenaar Arrangement[18] was the only transnational voluntary legal framework restricting the export of surveillance equipment, software and expertise.[19] In September 2020, the US State Department published a voluntary guidance for integrating UNGPs and more particularly HRDD in the export of surveillance technology,[20] the effectiveness of this document is unclear, given that it is neither comprehensive nor mandatory, and it is not meant to supersede existing export control regulations.[21]

6. On September 2021, building on the momentum for incorporation of mandatory HRDD requirements in the European Union,[22] a comprehensive EU-wide regulatory regime for export control of dual-use items became effective ('Recast Dual-Use Regulation').[23] The regulation

[14] 'Project Panoptic Has Partnered with Amnesty International & Article 19 to Launch #BanTheScan in India' (*Internet Freedom Foundation*, 11 November 2021) <https://internetfreedom.in/project-panoptic-has-partnered-with-amnesty-international-article-19-to-launch-banthescan-in-india/> accessed February 16, 2022.
[15] MP Sacco et al, "Ad Hoc Committee on Artificial Intelligence ('CAHAI'): Contributions to the Draft Feasibility Study on 'Human Rights Due Diligence for Artificial Intelligence'" (2022) <https://www.ibanet.org/MediaHandler?id=A1BDEB6E-6E38-4156-8416-E71A1ABF038D> accessed February 28, 2022.
[16] ibid 6-7.
[17] Office of the UN High Commissioner for Human Rights, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (28 May 2019, A/HRC/41/35) p. 7 <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx> accessed February 17, 2022.
[18] See: <https://wassenaar.org>.
[19] Heejin Kim, 'Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangular Dialogue' (2021) 70(2) International and Comparative Law Quarterly 379, 380 <https://doi.org/10.1017/S0020589321000105> accessed February 18, 2022.
[20] U.S. Department of State, 'Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities' (Bureau of Democracy, Human Rights, and Labor, September 2020) <https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/> last accessed February 17, 2022.
[21] Maria Pia Sacco, Theodora A Christou, and Anurag Bana, 'Digital Contact Tracing for the Covid-19 Epidemic: A Business and Human Rights Perspective' (*IBA Legal Policy and Research Unit*, 2020) p. 19 <https://www.ibanet.org/article/4b11819d-c580-47fe-b680-19bdbc201328> accessed February 17, 2022.
[22] Office of the UN High Commissioner for Human Rights, 'UN Human Rights "Issues Paper" on Legislative Proposals for Mandatory Human Rights Due Diligence by Companies' (June 2020) pp. 7-8 <https://www.ohchr.org/Documents/Issues/Business/MandatoryHR_Due_Diligence_Issues_Paper.pdf> accessed February 17, 2022.
[23] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) ('**Recast Dual-Use Regulation**').

applies to AI-based 'cyber-surveillance items' and is the EU's attempt to ex ante address adverse human rights impacts caused, contributed and/or linked to cyber-surveillance items.

7. Under article 3 of the Recast Dual-Use Regulation, cyber-surveillance items specifically designated as subject to 'dual-use' controls in Annex I require mandatory authorisation by Member State before export from the Union customs territory.[24] Furthermore, to combat risks from export of cyber-surveillance items *not listed in Annex I*, there are HRDD-based catch-all provisions which require an exporter to either: (i) seek authorisation before export, if competent authority informs exporter that such items are or may be used for violations of human rights;[25] or (ii) notify the competent authority if the exporter has 'reason to suspect', on the basis of the exporter's 'due diligence findings', of use or intended use of aforementioned items for violations of human rights.[26] The regulation underscores the importance of having 'ongoing effective, appropriate and proportionate' due diligence obligations, assessing risks related to the export of cyber-surveillance items on end-users and end-uses.[27]

8. Again, due diligence requirements are placed on other private sector actors including brokering services[28] and providers of technical assistance[29] of dual-use items listed in Annex I. Member States are also empowered to lay down 'effective, proportionate and dissuasive' penalties for those infringing the regulation.[30] What is important to note, however, is that the EU regulations do not prohibit export in dual-use items but merely restrict export subject to compliance with HRDD requirements. This is one way by which HRDD is being mainstreamed into the decision-making procedures of companies.

Theme 3 - Accountability and Remedy

A. Challenges for State-based Judicial/Non-judicial Grievance Mechanisms

1. Broadly, state-based mechanisms for accountability and remedy are piecemeal, with the *three* most widely relevant being - *data protection, cybersecurity (and cybercrimes)*, and *intellectual property*.[31] Furthermore, a major challenge for State-based judicial and non-judicial grievance mechanisms to provide accountability and remedy for human rights abuse related to technology companies is (i) the difficulty to identify the responsible actor(s) or (ii) the consequences of the abuse do not justify (individual) recourse through often costly proceedings in State-based mechanisms. For example, a person being discriminated against due to facial recognition by airport camera's involving the use of AI technologies may involve multiple responsible actors including the customs authorities, the producer, owner or user of the camera, the developer(s), user of the AI software, or the providers of the dataset the AI tool is trained with.

[24] Recast Dual-Use Regulation, art 3(1).
[25] Recast Dual-Use Regulation, art 5(1).
[26] See Recast Dual-Use Regulation, art 5(2).
[27] See Recast Dual-Use Regulation, art 2(32).
[28] Recast Dual-Use Regulation, art 6(2).
[29] Recast Dual-Use Regulation, art 8(2).
[30] Refer to Recast Dual-Use Regulation, art 25.
[31] For an overview of how these areas of law are relevant to disruptive technology including AI, see: Theodora Christou and Ian Walden, 'Legal and Regulatory Implications of Disruptive Technologies in Emerging Market Economies' (*SSRN*, 28 June 2018) <https://ssrn.com/abstract=3230674> or <http://dx.doi.org/10.2139/ssrn.3230674> accessed February 23, 2022.

2. This becomes further complicated if not all aforementioned entities are based in the country where abuse has taken place. Moreover, the indicated discrimination may result in an additional delay of an hour at customs. This may not be considered important enough to justify proceedings in State-based mechanisms. A comparable situation may arise when democracy is jeopardized by large scale abuse of sensitive data privacy, such as in the Cambridge Analytica scandal. This scandal resulted in neglectable damage at the individual level. Therefore, individuals may not be inclined to instigate proceedings for this type of abuse.

B. Proposed Solutions to Challenges for State-based Mechanisms

3. Solutions for these challenges can be developed in several directions. For example, one may solve the first issue (multiple potential perpetrators) by *reversing the burden of proof*. This may assist the victim because she may commence proceedings against one perpetrator and only if this entity is able to prove it was not responsible for, or has not contributed to the abuse, the claim may be dismissed. However, the victim then has to instigate new proceedings against the perpetrator and it is questionable whether she will engage in yet another proceeding, considering the cost issues. Besides, it is questionable whether States are willing to adopt this reversal of the burden of proof as they may be involved in the abuse themselves. Victims may commence proceedings against the entity most visible to them, in the given example customs. Beyond this, some adaptations may be made to international private law regulations in terms of jurisdiction over or applicable law regarding such abuses, enabling victims to instigate proceedings in the state in which the abuse has occurred. These adaptations are internationally sensitive and not easy to implement in existing frameworks.

4. A second solution may be to *open or incentivise collective redress against companies that cause large scale abuse involving limited damage on the individual level*. This solution performs best if the damage on the individual level is limited but is present. In such cases third-party funders or 'no-win-no-fee' arrangements tend to enable this kind of collective redress. However, if no individual damage can be proven, which may be the case in the Cambridge Analytica example, collective redress may not work, as no financial incentives are present for third-party funders or 'no-cure-no-pay' representation.

5. A solution in the latter situation, but also for other types of abuse, may be the *establishment of a public supervisor*, or *intervention by an existing public supervisor* which has supervisory powers regarding the abuse. Obviously, this requires legislation which imposes, for example, HRDD on tech companies. Public supervisors may usually intervene without any damage incurred by victims and have access to information even if a company is inclined to provide such information voluntarily. Often victims may request an investigation (and if appropriate, sanctioning of a company) by the public supervisor. If the supervisor refuses to investigate or sanction the company, a victim may file an administrative complaint and instigate proceedings at administrative courts, if this complaint is not resolved to their satisfaction. However, a public supervisor only has the power to investigate in its own country. Therefore, this investigation may be complicated if foreign entities, say, developers of AI, are involved. Collaboration between public supervisors may assist, but this may not be possible regarding all types of abuse, and heavily dependent on the State in which the relevant foreign public supervisor is based.

C. Persisting Issues with and Limitations of Proposed Solutions

6. Furthermore, human rights abuses may also amount to a criminal offence. For example, if AI software-based autonomous vehicles are developed that may cause physical damage, which is known to the producer but not remediated for economic reasons, this may amount to a criminal offence by the company or its board members.[32] If companies involved in these abuses (either through contribution or direct linkage) collaborate with the authorities (public prosecutor), to which extent is this contrary to the right not to incriminate oneself? For example, to what extent may the public prosecutor request information which the company has gathered in investigating its own matter, or in its ordinary HRDD process? Furthermore, the developer of the AI may not be based in the country in which the damage has occurred or the producer is based. If this necessitates collaboration with or prosecution by the authorities in another country, how does one prevent this prosecution itself resulting in human rights abuse of perpetrators? These are more common issues not restricted to tech, but deployment of tech may raise specific challenges as it may be unclear whether the AI software of the vehicle caused the problem or, any other software.

7. Finally, the potential issues are not only restricted to the *use* of technology but also their *creation*. Use of components or raw materials (eg, cobalt) used in tech appliances such as conflict minerals, the extraction of which frequently leads to human rights abuses is concerning.[33] Access to State-based mechanisms for such abuses in the respective countries it is taking place in, is often challenging, either because of cost of proceedings, a lack of trust, lack of access to relevant expertise or representation, as well as corruption. Therefore, access to State-based mechanisms in the countries in which the importers of such materials or the producers of the equipment are based may be more effective. The European Conflict Minerals Regulation[34] imposes duties on importers in the EU to conduct HRDD in this field and public supervisor may sanction perpetrators. However, access to these mechanisms by rights holders in distant countries is illusory without assistance by NGOs. That said, even with this assistance cost issues may arise and, obviously, not all affected rights holders will be assisted by NGOs. Likewise, complaints lodged against public supervisors of legislation implementing HRDD regarding their failure to investigate or sanction human rights abuses may also perform a role. However, this may trigger the challenges elaborated hereinabove, as the supervisor may not be able to investigate in the countries in which the abuse took place. Furthermore, rights holders will not have access to this type of complaint without assistance from an NGO either. In connection with this the abovementioned reversal of the burden of proof and adaptation of private international law regulations may also play a role.

[32] Whilst national laws are in place and regional instruments are being developed, including at the EU-level, the transnational issues remain. See, European Commission, Joint Research Centre, David Fernández Llorca, Emilia Gómez, *Trustworthy Autonomous Vehicles: Assessment Criteria for Trustworthy AI in the Autonomous Driving Domain* (2021) <https://data.europa.eu/doi/10.2760/120385> accessed February 23, 2022.

[33] A recent landmark case in the Democratic Republic of the Congo highlights some of the human rights issues. See: 'DR Congo Court Issues Rare Decision in Favour of Injured Worker at Cobalt Mine' (*RAID*, 22 February 2022) <https://www.raid-uk.org/blog/dr-congo-court-issues-rare-decision-favour-injured-worker-cobalt-mine> accessed February 23, 2022.

[34] Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas

Theme 4 - State's Duty to Protect, or Regulatory and Policy Responses

A. Existing State-based Attempts to Regulate AI

1. An example of the implementation in practice of pillar 1 of the UNGPs is the EU's proposed regulatory regime on AI - the Artificial Intelligence Act ('AIA').[35] The regulation is the first-ever comprehensive legal framework for this fast-developing area of technology. The AIA proposes the following risk-based categorisation of AI systems – *unacceptable risk, high risk, limited risk and minimal risk.* Each risk category is backed by commensurate regulatory obligations and restrictions. The AIA has extra-territorial reach since users of AI systems are covered by the regulations if they are located in the EU, irrespective of whether AI system providers are established within or outside the EU. AIA applies when the output produced by AI systems is used in the EU, even if the provider and user is established outside the EU.[36]

2. The AIA also proposes graded penalties such as – up to €30m or 6 per cent of global revenue (serious infringements), up to €20m or 4 per cent of global revenue (all other cases of non-compliance) and up to €10m or 2 per cent of global revenue (incorrect, incomplete or misleading information to competent authorities).[37] The AIA also proposes national-level AI supervisory authorities to supervise application of AIA along with a European Artificial Intelligence Board at the EU-level to support and guide the EC and national authorities in relevant matters.

3. Even though we welcome the attempt to regulate the risks of adverse human rights impacts associated with AI technologies, the four-pronged risk classification approach raises some concerns. In the first instance, it may lead to instances in which dangerous applications are wrongly classified as 'high-risk' when they should be 'prohibited' and thus are not subjected to proper oversight and safeguards. Lack of criteria for determining what should count as unacceptable risk lends to vagueness on how bright-lines have been drawn between prohibited and high-risk AI applications. In addition, this static classification of risks is not in line with the fast-evolving nature of AI-based technologies and with the dynamic nature of human rights due diligence, as defined by the UNGPs.

B. Proposed State-based Regulatory Solutions

4. It has been observed that more and more States are willing to enact binding instruments to ensure HRDD of AI systems. One proposed solution to address the lack of algorithmic transparency is 'Algorithmic Impact Assessment Process'. This impact assessment framework of accountability helps to engage public agencies and the public (individuals, communities, researchers, and policymakers) to participate in accountability efforts of automated decision systems before deployment through notice, comment, review, and due process elements. [38] On these lines, in its first federal legislative effort to regulate AI systems across industries, the U.S. is considering enactment of *Algorithmic Accountability Act 2022*. The proposed legislation will require the

[35] Proposal for a Regulation of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts Com/2021/206 Final <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206> accessed February 19, 2022 ('**AIA**').
[36] AIA, title I.
[37] AIA, title VI.
[38] Dillon Reisman et al, 'Algorithmic Impact Assessment: A Practical Framework for Public Agency Accountability' (*AI Now Institute*, 2018), see p. 7 onwards for elaborate discussion on elements of the algorithmic impact assessment process <https://ainowinstitute.org/aiareport2018.pdf> accessed February 19, 2022.

Federal Trade Commission (FTC) to develop regulations applicable to specified entities for conducting impact assessments[39] and meeting other compliance requirements[40] for automated decision-making systems. The Act has been welcomed as a positive development in the right direction by civil society organisations.[41] Alternatively, certain provisions in the recast dual-use regulations are case-in-point for *narrower* State regulation on individual AI-based items (like cyber-surveillance items).[42]

5. Another attempt was the proposed Algorithmic Fairness Act 2020 which sought to make the FTC to prevent covered entities from developing and implementing substantively and procedurally unfair algorithmic eligibility determinations for education, employment, credit, health care insurance, and housing.[43] Furthermore, in November 2021, New York adopted a law on 'Automated Employment Decision Tools' which requires 'bias audit' by independent auditor of algorithms which are used by employers in hiring or promotion. Employers are also required to notify job applicants when AI contributes in deciding who gets hired or promoted. And failure to comply with any provision of the new law leads to civil penalties.[44] However, its effectiveness in securing employer/employment agency compliance remains untested since the local law is to only take effect on 1 January 2023. Furthermore, regulations which clarify employer/agency obligations towards protected classes should be spelt out unambiguously to ensure effectiveness of the bias audit.[45]

*** * ***

[39] See generally Section 4 of the Algorithmic Accountability Act 2022, H.R.6580 – 117th Congress (2021-2022) <https://www.congress.gov/bill/117th-congress/house-bill/6580/text?r=2&s=1> accessed February 21, 2022.
[40] ibid see generally s 3.
[41] 'Algorithmic Decision-Making in the U.S. Needs Accountability' (*Access Now*, 3 February 2022) <https://www.accessnow.org/us-algorithmic-accountability-act/> accessed February 28, 2022.
[42] Refer to Q2, section (C) for discussion on EU regulation of cyber-surveillance items.
[43] See s 3 of the Algorithmic Fairness Act 2020, S.5052 – 116th Congress (2019-2020) <https://www.congress.gov/bill/116th-congress/senate-bill/5052/text#toc-H82D20B5D162B494F97F7B61E1B29BEE6> accessed February 21, 2022.
[44] Automated Employment Decision Tools 2021, 2021/144 <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=ID> accessed February 21, 2022.
[45] 'New York: Overview of the Automated Employment Decision Tools Law' (*Data Guidance*, 17 December 2021) <https://www.dataguidance.com/opinion/new-york-overview-automated-employment-decision> accessed February 25, 2022.