The Honorable Senator Eduardo Gomes
Rapporteur
Temporary Committee on Artificial Intelligence in Brazil
Federal Senate
National Congress Palace
DF 70 165-900, Annex 15th Floor
Brasilia

October 18, 2024

Re: Comments on AI Legislation – Proposed Substitute Text of Bill 2338/2023

BSA | The Software Alliance appreciates the opportunity to share our views on the Federal Senate's Temporary Committee on Artificial Intelligence's (CTIA) consideration of comprehensive AI legislation and, specifically, the proposed substitute text of Bill 2338/2023 released in the CTIA's latest interim report ("AI bill").

BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing cutting-edge services — including AI — and their products are used by businesses across every sector of the economy.[2] For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, cybersecurity services, and collaboration software. BSA members are on the leading edge of providing AI-enabled products and services. As a result, they have unique insights into the technology's tremendous potential to spur digital transformation and the policies that can best support the responsible use of AI.

BSA has engaged with Brazilian policymakers on a wide range of digital policy issues, including AI, data protection, cybersecurity, copyright, and procurement of cloud computing services. Notably, BSA presented to the Federal Senate's Committee of Jurists on AI as part of an expert private sector panel that provided insights on AI and submitted written recommendations to that committee on drafting AI legislation,[3] which it referenced in its final report. BSA also provided recommendations to Brazil's Ministry of Citizenship on clarifying that information analysis of data used to train AI systems is permissible under

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Cohere, Databricks, DocuSign, Dropbox, Elastic, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

[3] BSA, BSA Recommendations to the Jurists' Committee on AI for Effective AI Regulation in Brazil, *available at* https://www.bsa.org/files/policy-filings/en05302022airegbrazil.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

Brazil's copyright law,[4] and to the Ministry of Science, Technology, Innovation, and Communications on the development of Brazil's AI Strategy.[5] BSA has also engaged substantially with Brazilian policymakers on data governance issues more broadly, including providing legislative recommendations to the National Congress as early as 2017 on its consideration of data protection legislation[6] and, after the passage of Brazil's General Data Protection Law (LGPD), providing comments to the National Data Protection Authority, ANPD, on the law's implementation, including the regulation of international data transfers.[7]

BSA's views on AI policy are informed by our experience working with member companies to develop the BSA Framework to Build Trust in AI,[8] a risk management framework we published three years ago to help companies mitigate the potential for unintended bias in AI systems. Built on a vast body of research and informed by the experience of leading AI developers, the BSA Framework outlines a lifecycle-based approach for performing impact assessments and highlights corresponding best practices. BSA has testified before the United States Congress and the European Parliament on the Framework and its approach to mitigating AI-related risks.[9]

Our experience on these issues informs our recommendations to improve the draft AI bill.

I. Overview of BSA Recommendations

Brazil has undertaken significant efforts to become a global leader on addressing policy issues in the digital age, including by passing the Marco Civil da Internet in 2014, which aimed to ensure civil rights in the Internet age; strengthening privacy rights by enacting the LGPD in 2018 and subsequently amending the Federal Constitution to make data protection a fundamental right; and releasing national digital strategies – including the Brazilian Digital Transformation Strategy (E-Digital) and the Brazilian AI Strategy, which outlined an approach to stimulate trusted adoption of digital technologies and ethical AI innovation. The National Congress's myriad efforts to consider AI legislation buttress these policy initiatives and will have a significant impact on AI innovation.

CTIA's release of the draft AI bill is an important step toward achieving this goal. The draft AI bill aims to provide a comprehensive approach to AI by promoting transparency, protecting individual rights, ensuring human review, where feasible, requiring implementation of AI governance measures, identifying prohibited and high-risk uses,

---

[4] BSA, Submission of BSA | The Software Alliance to the Ministry of Citizenship Regarding the 2019 Review of the Brazilian Copyright Law, *available at* https://www.bsa.org/files/policy-filings/en08262019brazilcopyrightlaw.pdf.

[5] BSA, Comments on Brazil's National Artificial Intelligence Strategy, *available at* https://www.bsa.org/files/policy-filings/en02052020brazilaistrat.pdf.

[6] BSA Comments on Personal Data Protection Bill – PL 5276/2016, *available at* https://www.bsa.org/files/policy-filings/06052017BrazilPrivacyComments_en.pdf.

[7] BSA and Global Data Alliance, Response to ANPD Consultation on International Transfers, *available at* https://www.bsa.org/files/policy-filings/09262023intldatatrans.pdf.

[8] *See* BSA | The Software Alliance, Confronting Bias: BSA's Framework to Build Trust in AI, *available at* https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

[9] *See, e.g.,* Testimony of Victoria Espinel, Public Hearing on AI & Bias, Special Committee on Artificial Intelligence in a Digital Age, European Parliament, Nov. 30, 2021, *available at* https://www.europarl.europa.eu/cmsdata/244265/AIDA_Verbatim_30_November_2021_EN.pdf; Testimony of Victoria Espinel, The Need for Transparency in Artificial Intelligence, Before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Data Security, *available at* https://www.bsa.org/files/policy-filings/09122023aitestimonyoral.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001
P 202-872-5500
W bsa.org

imposing obligations on general purpose AI, creating a regulatory governance and enforcement framework, expanding protections for copyrighted information; addressing workplace issues, outlining measures to spur AI innovation, and promoting sustainable computing practices.

We appreciate CTIA's leadership in crafting legislation that aims to address an array of issues important to ensuring the responsible development and use of AI, but we are concerned that important parts of the draft AI bill would impede global interoperability, undermine Brazil's efforts to spur AI innovation, create significant compliance burdens, fail to delineate appropriate roles and responsibilities for companies along the AI supply chain, and create a fragmented regulatory enforcement framework. The bill would also have the unfortunate and unintended impact of limiting key insights that Brazilian government entities and Brazilian businesses can derive from AI tools, given that these tools require large and representative data sets that may include data that could be part of a copyrighted work, while at the same time expanding protection for that information in a way that departs from international norms. In light of these challenges, we propose recommendations below to better promote AI innovation and ensure individual rights.

Specifically, we recommend that the CTIA:

- Narrow the scope of uses classified as high risk;
- Enable companies to conduct internal impact assessments and protect them from public disclosure;
- Reconsider the sectoral approach to addressing key issues;
- Ensure obligations on AI actors fit the role;
- Revise the requirements for general purpose AI systems;
- Eliminate the AI incident reporting requirements;
- Revise enforcement approach by limiting the authority to conduct or order audits, removing the reversal of the burden of proof in civil actions, and decreasing fines; and
- Enable permissible use of copyrighted data for AI training, without mandatory remuneration to copyright holders or detailed disclosures on the use of copyrighted training data.

II. CTIA Should Narrow the Scope of High-Risk Uses

Policymakers around the globe have recognized the need to create guardrails around high-risk uses of AI. The draft AI bill appears to reflect this approach, primarily governing high-risk AI systems. However, its broad view of high-risk activities inadvertently sweeps in low-risk uses of AI. For example, in its classification of various employment practices as high-risk, the draft AI bill includes "distribution of tasks." Using AI to assist with scheduling workplace shifts or assigning new work projects based on availability poses few risks while yielding significant benefits – helping employers increase productivity and ensure their businesses can run smoothly. Such routine uses of AI should not be swept into regulation focused on high-risk uses of AI.

In addition, Article 14, section I of the draft AI bill refers to safety or security devices, depending on the translation, in the management and operation of critical infrastructure. It is unclear whether this applies to cybersecurity services, and we encourage CTIA to clarify that they are excluded from the scope of high-risk uses. AI is central to defenders' ability to protect our digital way of life from increasingly sophisticated cyber threats, and strong and effective cybersecurity defense relies heavily on its use. Policymakers should carefully

consider the varied nature of AI use cases to ensure that any new guardrails do not unintentionally inhibit the continued and expanded use of AI-powered tools for cyber defense. This approach would align with principles that both the Colorado AI law in the United States and Recital 55 of the EU AI Act have recognized. In fact, the latter expressly exempts cybersecurity as a safety component of critical infrastructure.

In addition to enumerating a list of high-risk uses in the draft bill, Article 16, section II authorizes the sectoral authorities to further define high-risk use cases based on several factors, including the "risk to the integrity of information." That standard is so broad that it could apply to every generative AI system which, even where testing demonstrates it performs at a high rate of accuracy, could invariably provide an inaccurate output and, consequently, violate the law.

Recommendation: We recommend that CTIA narrow both the scope of high-risk uses and the factors for specifying additional high-risk uses and clarify that cybersecurity services are not included within the scope of high-risk uses.

III. CTIA Should Revise the Impact Assessment Requirements to Ensure They Can Be Conducted Internally and Protected from Public Disclosure.

The draft AI bill imposes requirements on both developers and applicators to conduct preliminary risk assessments and algorithmic impact assessments, consult the public in preparing the impact assessments, provide the assessments to the competent authority, make the conclusions of the impact assessments public, and submit preliminary assessments to regulatory authorities with petitions that a risk should not be classified as high-risk. The draft AI bill further requires the competent authority to establish the criteria and frequency of updates for the impact assessments, consulting the other SIA entities, and create a publicly accessible database of impact assessment documents. As discussed below, the draft AI bill's approach to impact assessments undermines their effectiveness by requiring external disclosure and exposes sensitive proprietary business information.

A. Impact Assessments Should Be Part of Robust Internal Processes, Not Publicly Disclosed.

BSA supports policies that promote AI governance measures, such as impact assessments, which can ensure responsible development and use of AI. Impact assessments are important accountability tools that enable companies to identify and mitigate risks and are widely used in other fields, such as privacy, cybersecurity, and environmental protection. In the AI context, companies use impact assessments to examine key issues in the relevant stages of development and use – project conception, data acquisition, data preparation and model definition, testing, and operation monitoring.

The draft AI bill's approach to impact assessments undermines their utility and effectiveness, because it treats them as public documents rather than part of a robust internal assessment process. A key aspect of impact assessments is that that they require internal stakeholders – engineers, product development teams, and quality assurance teams – to thoroughly examine their assumptions, data handling practices, product features, potential impacts, and business processes, among other things, to identify where internal protocols and benchmarks have not been met, or potential risks have not been addressed, and further refine the product or service until it is appropriate to be placed on the market. This process, when conducted internally, enables rigorous analysis to vet all possible negative outcomes without fear of regulatory intervention or reputational harm.

Public disclosure of impact assessments or proactive disclosure to regulatory authorities would eliminate a key component that makes these assessments effective – their confidentiality. Disclosure – either to regulators or the public – discourages businesses from conducting internal inquiries with the same rigor and changes the nature of an assessment. When conducted internally, an impact assessment is focused on surfacing all possible negative outcomes, benefiting both companies and consumers. When conducted for purposes of public disclosure, the purpose of the assessment shifts to presenting a public-facing record that does not invite the same robust scrutiny.

Disclosure to external stakeholders also creates risks that sensitive proprietary business information will be revealed, which could adversely affect companies' competitiveness and undermine key business objectives. Impact assessments include an examination of sensitive commercial issues, such as detailed information about data assets and sources, in which companies make significant investments, and disclosing documentation assessing this information could put companies at a competitive disadvantage. The inability to protect the confidentiality of this information could also cause other significant harm. For example, in the cybersecurity context, it could provide a roadmap to cybercriminals on how to reverse engineer security protections.

These same confidentiality concerns apply to the draft AI bill's other disclosure requirements, including the requirement to allow public participation in the preparation of impact assessments, make conclusions of the impact assessments public, or create a publicly accessible database of impact assessment documents. These requirements risk divulging critical information that companies take significant efforts to protect.

B. CTIA Should Consider Alternative Approaches That Demonstrate Public Accountability While Protecting Sensitive Proprietary Information.

We support efforts for companies to demonstrate accountability to the public on their responsible development and use of AI and suggest alternative approaches that could help achieve that goal while also preserving the confidentiality of companies' sensitive proprietary business information.

- First, with respect to public participation, companies could solicit external feedback on the design of processes used to conduct impact assessments, which could facilitate the inclusion of a more comprehensive set of considerations, rather than facilitating participation in the actual preparation of the assessment, which involves an examination of sensitive information in which public access would not be appropriate.

- Second, companies can also voluntarily solicit external participation in other ways, such as consulting biological experts to evaluate the threat of misuse of an advanced model's capabilities to create biological weapons, or targeted affected stakeholders, where the product will be deployed in a specific or unique setting. However, the circumstances for when external consultation would be appropriate will vary significantly, and companies should maintain the flexibility to incorporate external feedback when they determine it is appropriate to do so, without inflexible legal requirements that apply a one-size-fits-all approach and may not be relevant for the specific use case.

- Third, in lieu of the disclosure-related and public participation requirements, the draft AI bill should allow companies to self-certify that they have conducted an

impact assessment, which they could maintain for a reasonable period of time – so long as it continues to serve a business purpose – in the event a regulator subsequently exercises its investigative authority to review a product or service. A public self-certification scheme assures key stakeholders that a company has taken the necessary internal steps to align its development and use of AI with industry best practices. In doing so, it both incentivizes more in-depth examinations that ferret out potential problems and protects sensitive proprietary business information contained in the assessments.

Recommendation: We recommend that CTIA delete all requirements from the draft AI bill that require public disclosure of impact assessments, proactive disclosure of impact assessments to government authorities, or public participation and instead require companies, based on their role, to conduct internal impact assessments and self-certify their compliance with this requirement.

IV. CTIA Should Streamline the Role of Sectoral Authorities.

AI is used across industry sectors, and stakeholders expect that regulators will continue to use their existing authority to address issues that fall within their domain. The draft AI bill contemplates an important role for sectoral authorities, who must, as mentioned above, specify high-risk uses of AI, receive and analyze algorithmic impact assessments, define the circumstances where algorithmic impact assessments will be streamlined, and regulate the criteria for and the frequency of impact assessments, among other things. The draft AI bill empowers the competent authority and the Permanent Council for Regulatory Cooperation (CRIA) to adopt common measures to guide the activities of the sectoral authorities.

Despite the creation of a coordinating function, and widespread recognition that sectoral regulation will invariably complement horizontal AI legislation, the draft AI bill's overreliance on sectoral authorities creates opportunities for inconsistent enforcement and unpredictable legal obligations. For example, the delineation of high-risk uses beyond those prescribed in the legislation not only makes it difficult for companies to understand what their legal obligations will be, and to make strategic investments and plan product development in line with those requirements, it also means that there could be significant variation in what those evolving requirements are based on the actions of each sectoral authority. This could pose an unwieldly compliance burden on companies and impose unintended costs that stymie technological development, frustrating the goal of spurring AI innovation.

The draft bill's failure to delineate the criteria for conducting impact assessments in the text of the legislation and delegation of key requirements – the criteria and frequency of impact assessments – to regulatory authorities creates similar concerns. As discussed above, impact assessments guide companies through a comprehensive process of considering a range of issues associated with product development and use, such as product features and capabilities or appropriateness of deployment settings. Understanding the criteria that will be included in these assessments is necessary to inform decisions about what products to place on the market, how to build them, and where to use them. The draft AI bill's failure to define these criteria further hampers companies' ability to predict what the legal obligations will be, which, as discussed further below, should be based on their roles. This uncertainty impedes the ability to conduct strategic planning, determine where to make investments, and make product development decisions.

Recommendation: We recommend that the CTIA streamline the responsibilities of sectoral authorities to ensure a more consistent approach across the Government of Brazil and define key obligations in the draft AI bill.

V. CTIA Should Ensure That Obligations Fit the Role of the Company in the AI Supply Chain.

The draft AI bill acknowledges that multiple companies comprise the AI supply chain, recognizing developers, "applicators," which are commonly referred to as deployers, and distributors. Any policies that create obligations for companies that design and use AI systems should reflect these different roles and assign obligations accordingly. Developers design or produce AI systems, and applicators use AI systems. Because of these different roles, their access to information and ability to identify or mitigate risks will vary based on their role. For example, developers will have access to information about how the AI system was initially trained, such as various aspects of the training data, including labeling techniques and types of data. Deployers, by contrast, will have more insight into the context in which that particular system is being used, and the decisions made based on that use, and are better positioned to monitor issues arising during deployment.

Despite these different roles, the draft AI bill misallocates obligations for the relevant actors in at least two circumstances: (1) requirements for impact assessments, which, as discussed above, are broadly delegated to regulatory authorities without specifications for creating role-based responsibilities; and (2) requirement for distributors to ensure compliance with governance measures, despite their lack of access to information to assess compliance.

A. The Draft Bill Should Require Impact Assessments to Reflect Role-Based Obligations.

Rather than leaving the criteria and frequency of impact assessments to regulatory authorities, the draft AI bill should clearly identify the requirements for companies to conduct impact assessments — and those requirements should reflect the different roles of developers and applicators. Currently, the draft AI bill does not direct the regulatory authorities to tailor the impact assessments based on the role of the company or otherwise suggest that these requirements should be different for the respective roles. It is therefore unclear whether regulatory authorities will consider this important issue when they are developing or updating impact assessment criteria.

Both developers and applicators should be required to conduct impact assessments, but the obligations should be based on their roles. In doing so, the CTIA can ensure that each actor has the ability to identify and mitigate the risk associated with the relevant stage of development or use over which they have control. As a result, we recommend, as noted above, that CTIA include the impact assessment criteria, based on the role of the actor, in the text of the legislation, but if it keeps the existing structure and delegates this responsibility to regulatory authorities, we recommend that it explicitly clarify that the competent authority must tailor the impact assessment requirements to the role of the company.

B. CTIA Should Delete Requirements on Distributors to Verify Developers' Compliance.

The draft AI bill also acknowledges the role of "distributors" of AI systems and imposes certain obligations on them. The draft AI bill defines a "distributor" as a person or entity that

"provides and distributes AI systems for third parties to operate" and requires them to ensure governance measures have been complied with before the product is placed on the market. As a threshold matter, it is not entirely clear what companies would be considered distributors, as the definition uses language that is so broad that it could encompass the original developer, a downstream company integrating a third-party AI model into its own software and providing it to a business customer – AI integrators – or an entity that makes no changes to AI systems but merely performs the business function of ensuring their availability to be licensed or sold on the market.

Nevertheless, to the extent that a distributor is an entity that is different than the original developer, it will lack access to the information necessary to verify whether the original developer has complied with the governance requirements. In addition to the lack of access to relevant information, a developer and distributor perform very different functions, and a distributor may lack the expertise and generally be ill-suited to assess the reliability or risks of the technology, given that their role is disseminating the product in the marketplace rather than creating the technology. As a result, the obligation on distributors to ensure the product's compliance with legal requirements before placing it on the market is misplaced.

Recommendation: We recommend that CTIA eliminate the requirement for distributors to ensure the product's compliance with governance requirements before placing it on the market.

VI. CTIA Should Revise the General Purpose Obligations

The draft AI bill also imposes several obligations on the developers of general purpose AI, including substantial obligations to anticipate and test for potential risks that would be beyond the knowledge of the developer. CTIA should revise the approach to general purpose AI systems to address two important issues: (1) the draft AI bill's departure from the risk-based approach; and (2) the need to ensure that the bill includes objective requirements that companies can implement in practice.

A. CTIA Should Revise Obligations on General Purpose AI

The draft AI bill largely focuses on high-risk uses of AI systems, but Section V's regulation of general purpose AI significantly departs from the risk-based approach. General purpose AI systems can be adapted for infinite uses, most of which are low-risk. Because of the multitude of possible uses, it is impractical to require companies to anticipate all potential uses across industry sectors. Notably, the draft AI bill not only seeks to regulate general purpose AI, as opposed to focusing exclusively on high-risk uses of AI, it also does not limit any of the general purpose AI obligations to models that pose systemic risks, as the EU does in its EU AI Act. Instead, it imposes all of the general purpose AI obligations on all types of general purpose models, without focusing on harms those requirements seek to address.

To the extent that CTIA retains general purpose AI obligations, we recommend it does not go beyond requirements that focus on transparency and information-sharing, consistent with those created in the EU AI Act for AI models that do not pose systemic risks.

Recommendation: If the general purpose AI obligations are retained, they should focus on information-sharing and transparency.

B. CTIA Should Revise the Generative AI Obligations to Enable Effective Implementation.

CTIA should also revise the generative AI obligations to make them more practical to implement. For example, the draft AI bill's requirement for generative AI developers to identify and mitigate risks to fundamental rights is broad and difficult to operationalize, particularly for models that may not ultimately be deployed in high-risk settings that implicate these individual rights. The requirement to identify and mitigate risks to the "democratic process" poses similar challenges and references issues beyond the developer's control. Legislation that creates concrete obligations that companies can implement in practice facilitates effective compliance, which enables the law to accomplish the goals it intends to achieve. As a result, we recommend that CTIA narrow the scope of the risks in Section V, Article 31.

Recommendation: CTIA should narrow the scope of the issues in the risk management requirements for generative AI developers in Section V, Article 31.

VII. CTIA Should Revise the Enforcement Provisions to Ensure a Balanced Framework.

The draft AI bill creates a robust enforcement framework, empowering regulators to conduct or order third-party audits; acknowledging the civil liability under other laws continues; reversing the burden of proof in those civil liability actions when the victim is "insufficient" or the operation of the AI system makes it "excessively burdensome" to prove the requirements for civil liability; and imposing significant fines, up to 2% of the gross revenue of the group or conglomerate in Brazil.

Strong enforcement is critical to ensuring that legislation is effective. We appreciate CTIA's focus on ensuring companies satisfy the law's obligations, but we also underscore the need for enforcement to not only be robust, but also balanced. An appropriate enforcement regime takes into account various considerations of the parties subject to penalties or regulatory or judicial oversight, including whether enforcement measures are fair or excessive. The draft AI bill's enforcement measures do not strike the right balance and impose overly burdensome obligations and excessive penalties.

For example, the competent authority's power to conduct audits is particularly invasive, because it can expose sensitive information. The draft bill does not reserve this significant power for violations of specific provisions, but rather treats it as a rather routine compliance assessment. The competent authority's power to order third-party audits is even less constrained, because it does not guarantee the confidentiality of sensitive proprietary business information, limit circumstances under which this power can be exercised, identify standards an audit must apply, or designate any framework that holds third-party auditors accountable. Similarly, the reversal of the burden of proof is a significant procedural change that could have an enormous impact on companies, but the draft AI bill would create a low threshold to trigger this reversal. Finally, the amount of fines – up to 2% of gross revenue – is also substantial and not proportional to the harms the law seeks to address.

Recommendation: CTIA should make the enforcement framework more proportionate by eliminating regulatory authority to conduct or order audits, deleting the provision reversing the burden of proof in civil actions, and decreasing the maximum amount of fines.

VIII. CTIA Should Eliminate the Incident Reporting Requirements.

Chapter VII of the draft AI bill requires AI agents to report "serious incidents" to competent authorities within a reasonable period of time. Those incidents include risk to human life, interruption of operation of critical infrastructure, serious damage to property or the environment, serious violations of fundamental rights, the integrity of information, and the democratic process. Section IV, § 6 separately requires AI agents that are aware of "an unexpected and relevant risk or impact" that AI systems on the market pose to individual rights to immediately inform competent authorities and the affected individuals.

We appreciate the focus on ensuring that companies identify and mitigate potential harms, which animates the incident reporting requirement. However, the draft AI bill's approach is flawed in several ways.

- First, incident reporting is not the best mechanism for addressing this challenge. AI is integrated into products and services across a variety of use cases, and AI's ubiquity means that incidents will often overlap with other critical areas already typically subject to reporting frameworks, like cybersecurity or critical infrastructure. This can create overlapping reporting requirement, which takes resources away from efforts to identify and remediate an incident.

- Second, the draft AI bill's threshold for incident reporting is overbroad, including fundamental rights, integrity of information, and the democratic process. It is unclear how AI agents will discern when incidents implicating these broader societal issues occurs and, even where that is the case, whether and how an AI system contributed to the incident.

- Third, the requirement fails to identify which entity along the value chain is responsible for reporting. The draft AI bill imposes the requirement on AI agents, which include developers, distributors, and applicators. However, these entities will have different access to information. In many circumstances, it is the applicator who will be best positioned to monitor when issues arise during use and understand the context that influences the severity of the risk.

- Fourth, the draft AI bill requires reporting to members of the public without regard to the feasibility or utility of this requirement. Unlike cybersecurity, where consumers might be instructed to download a patch to fix a software vulnerability, or a data breach where a consumer may be alerted to freeze their credit report, AI incidents may not arise in a context where a consumer can take action to limit potential harm. As a result, notifications to consumers would not serve a specific purpose. At the same time, this would require businesses to invest significant expense and resources to obtain the ability to identify affected stakeholders and communicate with them, in addition to creating privacy concerns about the need to collect personal information they may not otherwise have solely to fulfill this obligation. In light of the foregoing challenges, we recommend that CTIA eliminate incident reporting requirements from the draft AI bill.

Recommendation: CTIA should eliminate incident reporting requirements and, to the extent it retains these requirements, it should: (1) narrow the scope of the threshold to remove fundamental rights, integrity of information, and democratic processes;

(2) identify the specific entity responsible for reporting the incident; and (3) eliminate notification to affected stakeholders.

IX. CTIA Should Align the Copyright Portions of the Bill with International Best Practices

The draft AI bill requires AI developers to "inform" about any copyright-protected content used in training, as provided in regulations (Art. 60, page 62); does not grant legal permission to companies to engage in such training for commercial purposes (Art. 61, pages 62-63); and mandates that companies that use copyright-protected materials in the training of AI systems must remunerate the copyright owners for use (Art. 64, page 64-65).

We respectfully submit that each of these features departs markedly from prevailing practices adopted in other economies that are seeking to ensure that their governments, industries, and citizens can secure the benefits of AI.

- First, the proposed notification requirement regarding any potential copyright-protected content is not feasible to implement. Computational analysis is typically applied to a large training data corpus that may comprise millions or billions of tokenized data elements. Depending on how the model is trained, data accessible over the Internet may be collected as part of the raw data set that is transformed into that corpus. This raw data may include data that could be part of a copyrighted work because a substantial portion of the internet is potentially subject to copyright protection, which has a low threshold to establish originality and copyrightability. Everything from chatroom discussion to online social commentary to user-generated restaurant reviews are potentially subject to copyright. The vast extent of the universe of potentially copyrighted content and the difficulty in determining the provenance, scope of rights, and ownership of such content makes the notification obligation infeasible. As discussed below, this notification obligation is also inappropriate because computational analysis for AI training purposes is not a "consumptive" use of such content for its expressive purpose; rather it involves statistical analytics performed on data that itself is typically not subject to copyright, given that copyright protection does not extend to facts, ideas, or mathematical concepts.

- Second, the bill would create significant uncertainty regarding the legal permissibility of AI training for commercial purposes. Deterring and disincentivizing such AI training would be a major misstep that could undermine Brazil's competitiveness and innovative capacity in comparison with other economies that have not adopted such restrictions. As the government of Singapore noted in its 2019 Copyright Review Report,[10] copyright exceptions for AI training should not be limited to non-commercial activities for the following reasons:

  "Text and data mining is analogous to research work. Both activities involve obtaining data, manipulating and studying it, and coming to conclusions or discovering new ideas. ... [In the context of] research and study, ...whether an activity is commercial or non-commercial in nature is not always clear. It can start off as being non-commercial in nature but may evolve into activity of a commercial

[10] Singapore Copyright Review Report (2019), p. 32, at https://www.mlaw.gov.sg/files/news/public-consultations/2021/copyrightbill/Annex_A-Copyright_Report2019.pdf

nature. This also holds in the context of text and data mining activities. More importantly, as the purpose of text and data mining is to analyse data and not to consume what copyright seeks to protect (i.e. the creative expression of the copyright materials), it does not appear necessary to restrict uses that may not fall within or interfere with the copyright owner's normal exploitation of the materials in the first place – even if they are commercial in nature."[11]

- Third, the bill would allow any rightsholder to deny authorization to conduct AI training and/or would mandate remuneration for any use of data that may include part of a copyrighted work. We urge Brazil not to adopt this approach for several reasons. To begin, we urge Brazil to consider the potential impact on Brazil's own Artificial Intelligence Plan 2024-2028 – including its specific priorities relating to health, agriculture, the environment, industry, trade and services, and education – if AI training and R&D in these areas can so easily be impeded and subject to compensation demands of uncertain magnitude. We also urge Brazil to consider that such authorization and compensation frameworks will harm the ability of **Brazilian entities** to conduct AI training **in Brazil.** Finally, we urge Brazil to consider that AI training does not involve the consumption of any copyrighted works for their expressive content. Rather, such analysis involves mathematical calculations of probabilities, correlations, trends, and other patterns across the entire tokenized data set. Such analysis seeks to understand only the mathematical patterns (e.g., the relationships of specific tokens in relation to other tokens) distributed across the entire data set. These mathematical patterns are themselves not expressive content protected by copyright law.

- Fourth, we urge Brazil to take into account emerging global norms regarding the intersection of copyright and AI. There is an increasing global awareness about the need to modernize copyright laws to facilitate the development of AI, as illustrated below:

    - Japan: Japan first recognized such a need in 2009 when it amended its Copyright Act to create an explicit exception for reproductions that are created as part of a "computerized data processing." Although the 2009 amendment is heralded as having transformed Japan into a "machine learning paradise," the Japanese Diet codified a broader exception in 2018 that extends to "exploitation" of any copyrighted work for the purpose of performing "data analysis."

    - United States: In the United States, courts have confirmed that, under the "fair use" doctrine, incidental copies of a work made in the course of informational analysis are non-infringing, even where the analysis is performed for commercial purposes.

    - European Union: The European Union has passed legislation to provide clarity for the development of AI. Articles 3 and 4 of the Directive on Copyright and Related Rights in the Digital Single Market create two broad exceptions that authorize AI researchers to make reproductions that are needed for the purposes of carrying out "any automated analytical technique aimed at analyzing text and data in digital form in order to

[11] *Id.*

generate information which includes but is not limited to patterns, trends and correlations."

- Singapore: Singapore has adopted an exception in its copyright law that permits "computational data analysis" that involves the use of "a computer program to identify, extract and analyse information or data from [a]… Work."

Recommendation: We respectfully urge CTIA to take account of prevailing international practice, as well as a detailed assessment of Brazil's own national interest, in order to ensure that the Brazilian government, private sector, and citizenry will not be deprived of the benefits of AI due to a misapplication of copyright law norms. Among other things, we urge CTIA: (1) not to impose infeasible and overbroad obligations to provide information on copyrighted data used in training; (2) not to exclude from any copyright exception AI training conducted by a private entity or conducted for commercial purposes, consistent with other countries' and regions' adoption of such exception to facilitate the development of AI; and (3) not to adopt an authorization and compensation framework, which again, is out of step with prevailing international practice.

Thank you for the opportunity to share our views on the draft AI bill. We would be happy to continue to serve as a resource as you consider finalizing the bill.

Kind regards,

Shaundra Watson
Senior Director, Policy

Joseph Whitlock,
Director, Policy

Antônio Eduardo Mendes da Silva
Country Manager - Brazil