European Center for
Not-for-Profit Law

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

San Francisco, November 22, 2023

Re: White House National Security Council Roundtable on Artificial Intelligence

Dear Ms. Razzouk and Mr. Chhabra:

Thank you for inviting me to the White House National Security Council roundtable on artificial intelligence on November 14th. Following the in-person consultation, I'm sharing with you some initial written thoughts related to the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, as well as recommendations on the Biden-Harris Administration's international efforts related to AI governance.

The below recommendations and insights build on the European Center for Not-for-Profit Law's (ECNL) 20 years of work in enabling environment for civic space and participation. Since 2019, we've spearheaded work on digital rights and emerging technologies through substantial research and practical experience collaborating with civil society, AI developers and deployers, and policymakers around the world.

I look forward to engaging further with the U.S. White House, including the National Security Council. I'm based in San Francisco and am available to discuss or elaborate on any of the issues addressed in this paper. Please do not hesitate to contact me at marlena@ecnl.org.

Sincerely,

Marlena Wisniak

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

The need to take a human rights-based approach to AI governance.

This month, governments and international organizations have issued a flurry of legal and policy initiatives to regulate AI. As such, the US Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the EO on AI) falls within broader AI governance efforts. At ECNL, we especially welcome binding legal instruments like the EO, the Council of Europe Convention on AI, and the EU AI Act. Non-binding instruments such as the OMB Implementation Guidelines or the NIST Risk Management Framework can furthermore be of great value when concrete measures are aligned with international human rights and developed with meaningful participation of external stakeholders, including civil society.

Civil society and academics have documented extensively the harm that algorithmic systems already cause to people's rights today, especially to marginalized groups. While ECNL supports further research in understanding the human rights impacts of emerging AI models such as large language models (LLMs) and generative AI, we strongly encourage policymakers to focus on real-world harm and are pleased that the Biden-Harris Administration seems to be taking this approach. We therefore caution policymakers from diverting their attention solely to the so-called 'existential risks' of AI systems and use LLMs as an excuse to hinder legislative efforts.

Civil society and affected communities play a critical role in shaping international norms. We therefore urge policymakers around the world, including the White House, to meaningfully engage with them in developing and implementing AI regulation. This requires proactively asking for their input and providing in turn feedback on how this input was incorporated in the norms in an ongoing, iterative way.

The EO on AI: a welcome initiative if implementation thereof centers people's rights.

When delivering remarks at the UK AI Summit on November 1st, Vice President Harris assured that we need to create "a future where AI is used to advance human rights and human dignity, where privacy is protected and people have equal access to opportunity, where we make our democracies stronger and our world safer. A future where AI is used to advance the public interest." VP Harris repeatedly noted the key role that external stakeholders, especially civil society, play in this regard.

At ECNL, we're pleased that the Biden-Harris Administration is overall committed to taking a rights-based approach to AI regulation. This is visible in the EO on AI, which is structured around sector and context-specific provisions centered on people's rights to access justice, healthcare, housing, education, and employment.

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

We welcome the many provisions around risk prevention and mitigation, including specific metrics and requirements that can prevent risk mitigation measures from being performative and ineffective. We especially welcome and will follow the U.S. AI Safety Institute, as they create standards to test the safety of AI models for public use. We hope the standards will be rigorous and enable rights-based implementation of the EO on AI, understanding 'safety' as the protection and promotion of people's rights.

That said, we're concerned that the call for "more rapid and efficient contracting" can be misused to justify accelerated development and deployment of algorithmic systems, and we urge the U.S. government to interpret this narrowly. We believe that federal contracts are an important safeguard to incentivize AI researchers and developers to build rights-respecting AI, which should be prioritized over expedited contracting. We also welcome the mandate to OMB to provide recommendations for managing risk in federal procurement, and we encourage the OMB to include mandatory impact assessments. We're pleased that the OMB will develop a monitoring mechanism to ensure that procurement is aligned with its recommendations.

Furthermore, we caution against blanket claims that "AI is already helping the government better serve the American people, including by improving health outcomes, addressing climate change, and protecting federal agencies from cyber threats." The first questions to assess before developing, purchasing, or deploying algorithmic systems are: Who/which groups does this system help and who can it harm? Who defines the purpose of the AI system? What metrics are used to test their efficiency? What is the acceptable error rate and who defines it? What evidence is there that the AI system is necessary and leads to better outcomes compared to other systems? Is this the best use of public funds, and what funds are displaced for developing or using the AI system?

Our recommendations on the U.S. government's role in global AI governance:

1. Align domestic policy with U.S. agenda in international AI governance.

We encourage the U.S. government to continue actively taking part in ongoing multilateral initiatives to develop international norms around A from a human rights-based approach. Key initiatives that we recommend focusing on are the the Council of Europe Convention on AI (CAI), G7 Hiroshima process, relevant UN Human Rights Council and General Assembly resolutions, and the OECD AI principles.

Overall, we recommend focusing on legally binding instruments and regulation that leads to clear implementation or operationalization guidance, tools, methods,

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

and standards through mandatory measures, instead of voluntary high-level principles or ethical frameworks. This includes establishing expectations or clarifying broad transparency requirements on documentation, design, development, and use of AI models. Civil society should have the opportunity to meaningfully participate in regulatory and operationalization efforts; we urge the U.S. government to support, equip, and resource civil society, especially marginalized groups and those who don't traditionally engage in tech policy, to participate.

Regarding the Council of Europe CAI, we are deeply disappointed that the U.S. government is opposing immediate applicability of the Convention to the private sector, thereby severely hindering the Convention's effectiveness. Such a position puts the U.S. government at odds with its ongoing domestic regulatory efforts. By alienating its closest international allies and civil society, the U.S. is quickly damaging its credibility to advance public interest-driven AI regulation. We strongly urge the U.S. government to reverse its stance on excluding the private sector from the scope of the Convention. We further note that leaders in civil society and academia, including those that are observing parties, as well as the media are closely monitoring the U.S.'s role in the Council of Europe negotiations.

2. Develop international AI legal instruments as consistent with international human rights law.

International human rights law is a codified, universally accepted and overall implemented, and flexible framework that can be adapted to different contexts globally. It's also a well litigated instrument, with abundant case law that considers proportionality and balancing of competing interests when restricting rights, in line with the U.S. standard of compelling national interest. This is in stark contrast with vague and undefined concepts such as "values" or "ethics," which are driven by individual (generally corporate) actors. As the U.S. led the post- World War II efforts to codify international human rights norms globally, we call on the government to reestablish that baseline for global AI governance today. Finally, when AI systems are fundamentally incompatible with international human rights law, governments should prohibit their use.

3. Focus on real-world harm and adopt a sectoral approach to AI governance.

In line with the EO on AI and the OMB Implementation Guidelines, the U.S should actively participate in international efforts to ensure that AI is regulated from a sectoral approach focusing on justice, healthcare, housing, education, employment, and law enforcement. Regulation should furthermore be centered around preventing, mitigating, and remedying risks to human rights in these areas,

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

as opposed to an 'existential risk' of artificial general intelligence or emerging technology.

4. **Establish heightened obligations for the use of AI systems by law enforcement, including prohibitions.**

As consistent with previous State laws such as California, Oregon, Massachusetts, or Virginia, the U.S. government should push for prohibiting the use of AI systems that are fundamentally incompatible with human rights.

The U.S. government should call for a prohibition on biometric surveillance tools that have the capacity to identify, follow, single out, and track people everywhere they go. These include the use of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance in public and publicly accessible spaces by government agencies, emotion recognition, predictive policing, and biometric categorization based on protected characteristics such as race and ethnicity, gender, sexual orientation, or religion, among others.

When engaging in international efforts to regulate AI, the U.S. government should support banning such AI systems, without exemptions for law enforcement, criminal investigation, border control, counter-terrorism, or security agencies. Government agencies, especially law enforcement agencies, should also be prohibited from using and accessing data and information derived from the use of these technologies by private companies and other private actors.

In line with domestic laws and taking inspiration from the upcoming EU AI Act Annex 3, the U.S. should influence international negotiations to establish heightened obligations for sectors and actors where AI systems pose severe risks to human rights, such as the following:

- Law enforcement (e.g. for assessing risk, investigating, prosecuting, or profiling);
- Migration, asylum, and border control management;
- Administration of justice and democratic processes;
- Critical infrastructure;
- Educational and vocational training;
- Employment, including worker management systems such as recruitment, hiring, termination, and surveillance, and platform economy work;
- Access to and enjoyment of essential private and public services and benefits, including creditworthiness and insurance.

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

5. Push back against blanket exemptions for national security.

We urge the U.S. government to continue pushing back against blanket exemptions for national security or counter-terrorism purposes, as they've successfully done in the Council of Europe Convention on AI negotiations. The U.S. government should advance democracy and the rule of law, which are threatened by blanket exemptions, not least when such exemptions are instrumentalized by States with authoritarian practices to justify the unregulated use of AI.

Core international human rights treaties do not include blanket exemptions and instead provide exceptions and restrictions to human rights when strict conditions are met. In the case of AI systems, these would be satisfied where there is a legitimate aim to use the AI system, a legal basis; and the use is necessary and proportionate. Of note, the ICCPR acknowledges that national security can be a legitimate aim: using an AI system for this purpose thus remains possible where the other conditions are satisfied.

When engaging in international negotiations on AI governance, we therefore recommend that the U.S. government either a) not mention national security explicitly, leaving it to national courts to determine how to balance it as a legitimate interest with the protection of human rights and fundamental freedoms, as prescribed by the international human rights treaties; or b) refer to national security as a legitimate ground for *restrictions* in the legal instrument but requiring such restrictions to be clearly established by law and proportionate in a democratic society.

6. Ensure meaningful civil society participation in AI governance at the national and global level.

The U.S. governance should ensure, support, and resource civil society participation in AI governance efforts, especially marginalized groups and those who don't traditionally engage in tech policy. Domestically, this includes ensure the possibility to participate in *developing* AI technical standards such as any guidance that will result from the U.S. AI Safety Institute, NIST standards and frameworks. Globally, this means providing funding, resources, and support to participate in AI global standard setting processes such as the Internet Engineering Task Force (IETF) or the International Telecommunications Union (ITU).

Furthermore, the U.S. government should ensure that civil society can meaningfully participate, and is proactively included, in *implementing* AI laws, policies and standards globally. This includes highlighting the need for external stakeholder engagement in impact assessments, as well as putting pressure on AI developers and deployers to meaningfully engage with civil society at various

info@ecnl.org
0031 639029805
www.ecnl.org
@enablingNGOLaw

stages of the AI lifecycle. At ECNL, we've developed a methodology for meaningfully engaging stakeholders in AI development and use.[1] Our framework is based on consultations with nearly 300 experts and groups with lived experiences, and is currently being piloted with the city of Amsterdam as well as a U.S. social media company. We encourage the U.S. government to refer to and share this framework in their global AI governance efforts.

[1] ECNL, 'Framework for Meaningful Engagement' (2023), https://ecnl.org/publications/framework-meaningful-engagement-human-rights-impact-assessments-ai.