Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
Submission by Thorn, a Nonprofit Organization, in Response to the Office of Science and Technology Policy’s Notice of Request for Information on Public and Private Sector Uses of Biometric Technologies

Exhibited and potential benefits of a particular biometric technology:

Thorn welcomes the opportunity to provide information to the Office of Science and Technology Policy (OSTP) on some of the beneficial uses of biometric technologies to help inform the legislative framework surrounding them. Thorn is a non-profit organization that exists to build global technological solutions and infrastructure to combat child sexual abuse online. We believe in the power and potential of government, NGOs, and tech companies working together to eliminate child sexual abuse material (CSAM) online. This goal cannot be achieved by just one of these entities alone, and we appreciate OSTP’s collaborative national initiative to develop an Artificial Intelligence Bill of Rights.

As an organization with a mission to use technology as a force for good, one important consideration we want to ensure is taken into account as the Bill of Rights is crafted, is how these powerful technologies can be used to guard the privacy and safety of children. At Thorn, we believe that leveraging tailored and specific artificial intelligence-aided technology, on behalf of children, will help to ensure that they share in the benefits of technological innovation designed with their safety, privacy, and welfare in mind.

Unfortunately, anywhere there is a upload button, you will find users uploading child sexual abuse material. Online reports of this abuse material have increased by 15,000% over the last 15 years, and the privacy of child victims is violated every time content is shared.¹ At Thorn, we believe the only way to disrupt and end the proliferation of CSAM on the internet is through the proactive use of targeted technological solutions. To this end, we develop technological tools to stop the spread

¹ National Center for Missing & Exploited Children, Key Facts
of abusive content by quickly identifying, removing, and then reporting CSAM from online platforms.

In the space of child protection, there are well established technologies that have been tested and refined for over a decade, but many of the most cutting edge technologies still need the space for further innovation. These technologies have proven results of finding and saving children from online sexual exploitation. Tailored technological solutions in this space are the future of protecting children from online exploitation, and there needs to be a legislative framework that allows for this crucial work to continue. We understand the concerns that some AI applications could lead to the invasion of individual users' privacy, but child advocacy organizations have always worked towards surgical and balanced solutions in order to protect children online.

Technology constantly changes and improves with time, and we believe that any legislative framework must reflect this reality. If regulation becomes indiscriminate, or does not provide the necessary flexibility for this specific use case, it can create unintended consequences that could deter the development of new technologies with the potential to protect children online. Because of this, legislation around artificial intelligence must allow for innovation and growth of preventative tools and measures developed to safeguard children from online sexual abuse.

For example, through the use of targeted biometric technology, an investigator could potentially identify a child whose abuse images are circulating online, because that technology is capable of identifying the child's specific body markers. There have been cases of some of the most egregious child sexual abuse where a child or perpetrator has been identified through distinct body marks - whether it be tattoos, birthmarks, etc. Without this flexibility to innovate, perpetrators will be able to utilize the most sophisticated technology to abuse children, while the child protection ecosystem falls behind.

Another example of how AI can be effective in this space is through the development and deployment of classifiers that are trained on data to make predictions and decisions on new data. And, as online platforms continue to share data, users can fine-tune the models to improve predictions over time.

Our image based classifier is deployed to find new and unknown CSAM. This classifier
is based on a machine learning algorithm we created, and has been trained on known CSAM, benign imagery, and adult imagery data sets in order to make it highly accurate and precise at identifying CSAM. Identifying new CSAM at scale ultimately helps in the identification and rescue of children and stops the viral spread of abuse on the open web.

Similarly, our text analysis classifier was developed to help prevent the grooming of a child for abuse. Through pairing the latest research from the child safety ecosystem with state of the art Natural Language Processing tools, our text-based classifier detects potential instances of grooming for sexual exploitation. This classifier is able to give predictions for specific lines in conversations that could indicate grooming, enabling quick review for human moderators, and empowering online platforms to automate the detection of grooming conversations in real time. Effective grooming detection is a crucial step in preventing child sexual abuse from happening in the first place. It can mean the difference between exploitation happening or not, again, intercepting before the abuse happens.

These targeted, surgical detection methods have been designed solely to combat child sexual abuse and grooming, and maintaining the use of these methods gives consumers the privacy that is expected without enabling bad actors and online predators. The spread of CSAM will never end if we are unable to create and deploy preventative tools and measures.

Child sexual abuse detection technologies are cutting edge and designed to protect the most vulnerable population in our society. Given this sensitivity, we acknowledge that safeguards and greater transparency are necessary for artificial intelligence technology used in this space. Any artificial intelligence regulation must find a balance that protects the general consumer’s privacy while still allowing for technology designed to protect children. We must not allow offenders the ability to reverse engineer technologies designed to keep our children safe. Any enhanced transparency should not impede the development of technologies that are used to protect children online.

We recommend that artificial intelligence-aided child sexual abuse detection methods be preserved, prioritized, and future-proofed in any legislative proposals around these powerful technologies. Recognizing that much of the narrative surrounding these technologies often centers on the potential harms of artificial intelligence and
biometric technologies, we hope the Office of Science and Technology Policy will also prioritize the benefits of these technologies on behalf of our children. In the same way we want to ensure these technologies do not overstep or abuse the rights of any person, they also should be utilized to protect the basic rights of our children to not be sexually abused or harmed. They are the future.

Thorn looks forward to serving as a resource to the Office of Science and Technology Policy regarding how we use biometric technologies to help reduce the spread of child sexual abuse material and to prevent child sexual exploitation.