Dear Office of the High Commissioner for Human Rights,

Thanks for your kind attention.

I am a computer science student studying the Basics of Cryptographic Systems at Brown University. I'm writing to respond to the call for input: "The relationship between human rights and technical standard-setting processes for new and emerging digital technologies (2023)" - Report of the High Commissioner for Human Rights

My submission focuses on 2 particular sub-topics under the guiding questions:

- How do technical standards for new and emerging digital technologies impact the enjoyment of human rights; what are related risks and opportunities?
- What are the duties and responsibilities of standard-setting organizations and their stakeholders in effectively integrating human rights considerations in technical standard-setting processes for new and emerging digital technologies?"

Through learning about cryptographic systems, I realized that there's a need for more diversity and open resources in highly technical fields such as cryptography and cybersecurity. The current talent pool in the field is very uniform. Since the people who invent cryptographic systems have the power to make decisions on who has access and who shares authority, it's risky for human rights protection. The fact that such important decisions are made by an elite small group of people can cause potential problems. I learned that the people who create these systems including mathematicians, engineers, corporations, and government agencies are mostly made up of elite professionals living in North America and Europe. Security should be an open resource, and when the power is controlled by a very homogenous group, there will potentially be problems related to human rights.

Therefore, I believe it's necessary to level the playing ground of highly technical areas like cybersecurity so that human rights can really be protected. Making emerging technology fields more diverse will help to protect human rights in general. Another solution to tackle this issue is to make the implementation and standardization of cryptosystems more "open" and healthy by making education and knowledge accessible to the public.

I also believe that corporations, especially standard-setting organizations, are responsible for building a healthy environment because they are often the pioneers in their relative technology fields.

A particular example is Cryptosystems which is constantly improving and evolving. Oftentimes, it's the larger corporations that benefit from the work of new technologies given their abundant resources and talents. One particular example in cybersecurity is the discussion of post-quantum cryptography which is the prevention of possible quantum computer attacks which is still not advent yet. The most recent submission is the fourth round from July 2022 as seen on the computer security resource center(https://csrc.nist.gov/projects/post-quantum-cryptography). There were only a total of 4 submissions. Interestingly, one of them named "Bike", Bit Flipping Key Encapsulation, could be supported by Google. Another project to note is HQC, Hamming Quasi-Cyclic, which states that it provides "security against attacks by both classical and quantum computers". Reading through the teams of these projects, I noticed that all of these have connections to large corporations and are all based in North America and Europe. I believe it's critical to the protection of human rights to have more diverse groups of talent in emerging technology fields to prevent the concentration of power onto a few corporates and a few groups of people.