University of California, Berkeley

AI and The Human Rights of Privacy:

What Clearview AI v ACLU Can Teach Us About the Future of Privacy Rights in International

Human Rights Law

Hanan Coronado

29 November, 2023

As the influence of artificial intelligence intensifies on the global stage, the importance of upholding human rights in the face of AI's unprecedented evolution has reached a critical point. The contemporary challenge of preserving anonymity has become increasingly difficult as technology companies advance their ability to track and surveil individuals through artificial intelligence-based facial recognition technologies, ultimately disempowering individual users and consumers. This erosion of privacy directly contradicts international human rights standards. A case exemplifying this threat is the legal confrontation between Clearview AI and the American Civil Liberties Union (ACLU), wherein Clearview AI, a tech entity, amassed and sold approximately 10 billion images scraped from online sources by 2021 (Dul, 1). Although Clearview AI settled its lawsuit with the ACLU by committing not to sell its facial recognition data to private companies, the threat of privacy violations in the artificial intelligence era symbolizes one of the most formidable challenges to human rights today. Although the right to privacy is underscored under the *International Covenant on Civil and Political Rights under International law* and corporate responsibility under the *Guiding Principles of Business and Human Rights*, explicit language should be developed to consolidate a general framework around AI and privacy rights, offering protection against exploitative practices of tech companies. The Clearview AI v ACLU case highlights the threat that surveillance mechanisms pose to vulnerable populations, necessitating the development of a more robust legal framework under international human rights law to safeguard privacy rights and hold tech companies accountable for potential human rights violations arising from the advancement of artificial intelligence. *International Human Rights Law can help develop a general framework that prevents companies like Clearview AI from infringing upon the right to privacy by building upon existing human rights treaties.*

Privacy is a right explicitly protected under international Human rights law; nevertheless, there is currently a lack of language focusing on the implications of AI under any global framework. The absence of clear, internationally consolidated AI guidelines has led companies like Clearview AI to have a market-driven approach to ethics in their technology, resulting in exploitative and non-consensual data collection. The danger of Clearview AI was brought to the forefront of mainstream media by the *New York Times* in 2021, exposing its facial recognition app that can erode privacy as we know it (Hill). Clearview AI is a company that profits from harvesting data through a facial recognition application and storing it in a database, collecting photographs of individuals from all over the internet without their consent (Dul 1). According to a complaint filed by the ACLU, Clearview AI sold these images to over 200 companies, encompassing giant corporations like Walmart and Bank of America, but not excluding celebrities and wealthy individuals with the money to access this sensitive information (*ACLU v. Clearview AI*). The company initially stated that its data was only being sold to the US and Canadian governments; however, in 2022, it admitted that it was also being sold to private companies and other individuals (Dul 2). This facial recognition tool harms vulnerable individuals' privacy and safety by making their identities available to anyone accessing its database, violating their fundamental right to privacy. In its complaint, the ACLU underscores the critical need to protect the privacy rights of survivors of sexual and domestic violence. It emphasizes the vulnerability posed by the potential exposure of sensitive information that could reveal their identities, highlighting the significant threat posed by facial recognition technologies (*ACLU v. Clearview AI*).

This lucrative data scheme violates the International Covenant on Civil and Political Rights when interpreted to protect against data collection, thereby ensuring the right to privacy

within the broader International Human Rights legal framework. Article 17 of the ICCPR states,

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home,

or correspondence" (United Nations Article 17). The right to undisturbed privacy should

encompass autonomy over one's data when utilized by private entities, especially when the

specific nature of their use remains undisclosed. The ICCPR should work to impact AI ethics

significantly by holding all participating parties accountable to its guiding legislation; however, it

is not specific to the modern privacy challenges of revolutionizing technologies (Kohn 202).

Clearview AI blatantly infringes upon individuals' privacy rights by neglecting to seek their

consent and capitalizing on collecting their digital data. However, the overly brief language

under Article 17 renders it insufficient for holding tech companies accountable. The U.N. Human

Rights Committee should play a pivotal role in formulating new interpretive comments that

mandate explicit consent for data collection within the framework of Article 17. These guidelines

would inform nations to develop their data privacy policies, leading to more accountability for

companies like Clearview AI (Kohn, 233).

Furthermore, a report by the Special Rapporteur on promoting and protecting the right to

freedom concerning cyberspace explicitly warns against the inadequate protection of the right to

privacy. The document states that "there are insufficient or inadequate data protection laws in

many states stipulating who is allowed access to personal data" (*United Nations*) while noting

that privacy rights are protected under the ICCPR. The document calls on states to create laws

ensuring citizens' data are safe from arbitrary surveillance from state or private entities.

However, without a clear international guide on AI, states are left to develop their own legal

framework around privacy and AI. This presents challenges in addressing human rights

violations of privacy by multinational corporations, particularly in the evolving AI arms race,

which has prompted competing countries to disregard harmful AI systems (Scharre, 135). Countries are eager to develop AI systems like Clearview AI that harness unprecedented benefits to things like criminal justice and government services, but by doing so, they fail to ensure that tech mechanisms are safe. Anna Su describes the AI nationalism phenomenon and characterizes it as a new type of geopolitics that can have long-lasting consequences for human rights. She further asserts that the asymmetry of AI-capable and non-AI-capable states presents a potential human rights issue that can only be addressed by International Human Rights Law (Su, 171). The human rights of AI are unconsolidated internationally, and even domestic law regarding AI is unclear. Taking the case of Clearview AI, the lack of a national legal guide to AI responsibility promotes the ill use of AI companies. The answer to AI technologies in the US is an example of a legal patchwork hindering determined responses to companies like Clearview (Dul, 14). Without a cooperative framework for dealing with emerging AI technologies and their implications on privacy rights, it is difficult to seek justice against malicious uses of data from companies like Clearview AI.

The development of AI places a paramount responsibility on corporations to safeguard privacy rights, given the ambiguous international human rights guidelines defining their role. In 2011, UN Special Representative John Ruggie led the development of the *Guiding Principles on Business and Human Rights,* mandating private entities to protect, respect, and remedy human rights (*United Nations*). The document asserts that business enterprises' responsibility to respect human rights encompasses internationally recognized human rights (*United Nations*), emphasizing adherence to standards like the ICCPR. These guidelines obligate corporations to proactively prevent and abstain from activities that infringe upon fundamental human rights, underscoring the grave societal impact of their actions.

While an international AI case has yet to be witnessed due to the lack of specificity in human rights law, assigning a more AI-specific responsibility to tech companies could enhance their accountability as they continue to dominate the global market. The case of Clearview AI was regional, but its effects extended beyond the U.S. and triggered legal retaliation in Canada by the Office of the Privacy Commissioner, as discussed in the Queen Mary Journal of Law (Dul 15). Tech companies like Clearview AI increasingly influence privacy rights on a multinational scale, necessitating a comprehensive guideline to steer nations and hold companies legally accountable for international violations. A cooperative AI Human rights business framework could prevent emerging tech companies from infringing on vulnerable people's rights, such as plaintiffs in the ACLU v Clearview AI case, regardless of their location in the world. According to the Nordic Journal of Human Rights, international AI initiatives require further development of AI-specific guidance on Human Rights Due diligence (Lane, 315). The existing Guiding Principles, designed for businesses of all sizes and types, lack clarity in the context of AI (Lane 310). Consequently, transnational technology corporations have addressed AI ethics through internally crafted principles and statements guided by the belief that AI governance should be market-driven and self-regulated (Su, 169). International Human Rights Law can effectively mold AI's normative values and function as a crucial corporate oversight mechanism (Su, 171). A consolidated international human rights guiding statement will ensure that the most affected communities have a voice in advocating for their right to privacy against tech monopolies.

The escalating influence of technology companies such as Clearview AI presents a substantial threat to human rights globally, with the potential to disproportionately affect marginalized communities within an inherently unequal power dynamic. The rapid advancement of artificial intelligence demands a concerted global effort to establish a comprehensive legal

framework capable of holding both states and private entities accountable for the human rights implications arising from emerging technologies. The Clearview AI v ACLU case is a stark illustration of the pressing need for an expanded legal arsenal within international law to address the complexities introduced by AI. The resolution of the lawsuit through an agreement, without any legal consequences for Clearview AI, underscores the existing challenges in ensuring accountability in artificial intelligence. While the International Covenant on Civil and Political Rights (ICCPR) and the Guiding Principles on Business and Human Rights offer a foundational framework for addressing AI accountability on a global scale, there is a clear imperative to refine and enhance their language to encompass the unique challenges posed by artificial intelligence explicitly. To safeguard human rights in the face of evolving technologies, the international community must collaborate to strengthen legal mechanisms, ensuring that the ethical implications of AI are adequately addressed. The Clearview AI case serves as a critical reminder that the ongoing evolution of technology demands proactive and adaptive measures within the international legal landscape to uphold the fundamental right to privacy in the age of AI.

Works Cited

"ACLU v. Clearview AI - Complaint." *American Civil Liberties Union*,

    www.aclu.org/legal-document/aclu-v-clearview-ai-complaint. Accessed 29 Nov. 2023.

Dull, Camilla. "Facial Recognition Technology vs Privacy: The Case of Clearview AI." *Queen*

    Mary Law Journal, 2022, p 1-24. HeinOnline.

    heinonline.org/HOL/Page?handle=hein.journals%2Fqmlj2022&collection=journals&id=

    11&startid=&endid=34.

Kohn, Miriam. "Clearview AI, TikTok, and the Collection of Facial Images in International

    Law." Chicago Journal of International Law, vol. 23, no. 1, Summer 2022, pp. 195-234.

    HeinOnline.

    https://heinonline.org/HOL/Page?handle=hein.journals/cjil23&collection=journals&id=1

    99&startid=&endid=238

Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York*

    Times, The New York Times, 18 Jan. 2020,

    www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Lottie Lane (2023) Artificial Intelligence and Human Rights: Corporate Responsibility in AI

    Governance Initiatives, Nordic Journal of Human Rights, 41:3, 304-325, DOI:

    10.1080/18918131.2022.2137288

Scharre, Paul. "Killer Apps: The Real Dangers of an AI Arms Race." *Foreign Affairs*, vol 98, no.

    3, 2019, pp 135-144. Heinonline.

    heinonline.org/HOL/P?h=hein.journals%2Ffora98&i=557.

"Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of

   Opinion and Expression, Frank La Rue." *United Nations*, United Nations,

   digitallibrary.un.org/record/730906?ln=en. Accessed 29 Nov. 2023.

United Nations, General Assembly. International Covenant on Civil and Political Rights. *Treaty*

   Series, vol. 999, Dec. 1966. *United Nations*,

   https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.

   pdf

United Nations, *The UN Guiding Principles on Business and Human Rights and... - OHCHR*,

   www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesB

   usinessHR.pdf. Accessed 30 Nov. 2023.