ICNL

www.icnl.org
info@icnl.org

PRESENTED TO OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS

SUBMISSION

The Impact of Artificial Intelligence Technologies on the Right to Privacy and Civic Freedoms

Introduction

This submission by the International Center for Not-for-Profit Law (ICNL) is in response to the call for input on "the right to privacy in the digital age" by the Office of the High Commissioner for Human Rights (OHCHR). The submission focuses on Question 1(e), the interlinkages between the promotion and protection of the right to privacy in the context of the use of artificial intelligence (AI) and the exercise of other human rights.

The increasing proliferation of AI technologies poses a threat to the right to privacy and an array of intrinsically connected civic freedoms, including the right to free assembly, association, and expression. Due to a lack of robust safeguards enshrined in laws, regulations and policies, AI systems are already being used to restrict the exercise of fundamental human rights. These restrictions are likely to increase without strong international standards and protections.

As noted by the former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, despite the widespread recognition of the right to privacy, the interpretation of this right "… raises challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest."[1] The Special Rapporteur defined the right to privacy as "…the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[2] The right to privacy includes "…the ability of individuals to determine who holds information about them and how is that information used."[3]

With the ever-increasing presence of digital technologies in daily life and the confluence of the physical and virtual worlds, an individual's private sphere extends beyond their physical private space. The right to privacy necessarily places the individual at the forefront; it is up to her or him to determine who possesses information about her or him and how that information is used. Unfortunately, AI systems not only rely upon vast amounts of public and private data for their development, but are also being deployed in ways that rupture the

[1] United Nations Human Rights Council, A/HRC/23/40, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 21.
[2] *Id.* at para 22.
[3] *Id.* at para 22.

'private sphere,' which in turn restrict the ability of people to exercise the freedoms of assembly, association, and expression.

In this submission, we highlight a few select issues that are illustrative of how AI systems violate the right to privacy and restrict civic freedoms. These examples demonstrate the need for international standards that will safeguard the right to privacy in the digital age.

AI Technologies and the Impact on Privacy and Free Assembly

The use of facial recognition technology in the context of protests and assemblies facilitates identification and punishment, directly impinging on the rights to privacy and free assembly.

Freedom of assembly is intrinsically connected with the right to privacy.[4] Facial recognition technology has been increasingly utilized by states to surveil and track their citizens, whether indirectly for the purposes of national identity systems[5] or crime reduction,[6] or more explicitly to track dissidents. The latter results in violations of individuals' right to privacy and right to free assembly by allowing authorities to identify and punish persons participating in peaceful protests. Even where this technology is used for seemingly innocuous purposes, there are concerns related to the use of individuals' data and privacy, as well as how their information might be used to restrict other rights. For example, in the context of the COVID-19 pandemic, various applications that utilize AI have been used to identify and track the spread of the virus and help monitor compliance with social distancing rules by tracking crowd formations, among other uses, and clear oversight over the collection and use of personal data from these applications is lacking.[7] In the Philippines, which implemented the use of a contact tracing app as a requirement for entry into government and private establishments, there were significant concerns around the use of this app for non-pandemic-related surveillance in light of a broader context of crackdowns on civil society and red-tagging of activists.[8]

In several instances, authorities have used facial recogniztion to identify, harass and arrest peaceful protestors. In Hong Kong, facial recognition technology has been used by

[4] United Nations Human Rights Council, A/HRC/41/41, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule" May 17, 2019, para. 16.
[5] *See, e.g.,* Reuters, *Singapore's use of facial verification in ID scheme stirs privacy fears,* Sept. 2020, https://www.reuters.com/article/singapore-tech-facialrecognition/singapores-use-of-facial-verification-in-id-scheme-stirs-privacy-fears-idUKL8N2GO0AS; Biometric update.com, *Philsys Digital Identity Registration System To Be Fast-Tracked*, May 2021, https://www.biometricupdate.com/202105/philsys-digital-identity-registration-system-to-be-fast-tracked
[6] *See, e.g.,* Vice, *Authorities Are Installing Recognition Surveillance Cameras All Over Manila*, March 2020, https://www.vice.com/en/article/k7exam/authorities-installing-facial-recognition-surveillance-cameras-manila-privacy-concern; BBC, *Met Police to deploy facial recognition cameras,* Jan. 2020, https://www.bbc.com/news/uk-51237665
[7] Lexology, *COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic*, https://www.lexology.com/library/detail.aspx?g=0d657003-bccc-44c1-8bb9-351ab28b3d04
[8] *See, e.g.,* Rappler, *Gov't goes full-throttle on StaySafe app, but user data concerns remain*, Dec. 2020, https://www.rappler.com/newsbreak/in-depth/government-full-throttle-staysafe-app-questions-remain-users-data; Rappler, *Leftists, activists dare Duterte gov't: Back claims of red-tagging with 'credible proof,'* Nov. 2020, https://www.rappler.com/nation/leftists-activists-dare-duterte-government-stop-talk-show-proof-red-tagging

the police to identify individuals protesting against the passage of the 2019 Fugitive Offenders and Mutual Legal Assistance in Criminal Matters Legislation Bill (the Hong Kong extradition bill) for arrest.[9] In India, the Delhi police have used facial recognition technology to identify individuals who participated in the 2019 protests against the Citizenship Amendment Act and more recently individuals participating in the ongoing farmer protests.[10] In the United States, facial recognition technology has been used by federal and local authorities to identify and target peaceful protesters, including those who participated in Black Lives Matter protests.[11] In Russia, the police used facial recognition technology to identify and subsequently detain activists and journalists who attended a peaceful rally in support of Aleksei Navalny.[12]

Not only does the use of facial recognition technology during protests violate the rights of individuals to privacy and free assembly during the assembly, it also results in continued violations of the right to privacy and other rights after the assembly. For example, in the case of Derrick "Dwreck" Ingram, co-founder of the social justice organization Warriors in the Garden who participated in a Black Lives Matter protest in New York, police officers used facial recognition technology to match Dwreck to an Instagram photo. The police then attempted to arrest Dwreck and break down his door on the basis of this photo, and placed "Wanted" posters around his neighborhood that were created using photos from Dwreck's private Instagram account without his consent.[13] Such violations of the right to privacy and free assembly also have a broader chilling effect on assembly by introducing the threat of identification and punishment. In most contexts, the use of facial recognition technology has been implemented without citizen input—or even awareness—and a regulatory framework articulating the permissible uses and limits of such technology and ensuring compatibility with human rights standards does not exist.[14]

---

[9] NY Times, *In Hong Kong Protests, Faces Become Weapons,* July 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html

[10] See, e.g., Business Insider, *India is ramping up the use of facial recognition to track down individuals without any laws to keep track of how this technology is being used*, Feb. 2021, https://www.businessinsider.in/tech/news/what-is-facial-recognition-technology-and-how-india-is-using-it-to-track-down-protestors-and-individuals/articleshow/80782606.cms; Financial Times, https://www.ft.com/content/044add20-7129-44a8-bc9d-92919a73d049

[11] Amnesty International, *Ban dangerous facial recognition technology that amplifies racist policing*, Jan. 2021, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

[12] Amnesty International, *Russia: Police target peaceful protesters identified using facial recognition technology*, April 2021, https://www.amnesty.org/en/latest/news/2021/04/russia-police-target-peaceful-protesters-identified-using-facial-recognition-technology/

[13] Amnesty International, *Ban dangerous facial recognition technology that amplifies racist policing*, Jan. 2021, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

[14] *See, e.g.* Amnesty International, *Ban dangerous facial recognition technology that amplifies racist policing*, Jan. 2021, https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/; ACLU, *The Government Has a Secret Plan to Track Everyone's Faces at Airports. We're Suing, March 2020, https://www.aclu.org/news/privacy-technology/the-government-has-a-secret-plan-to-track-everyones-faces-at-airports-were-suing/*; Aljazeera, *Privacy fears as India's gov't schools install facial recognition*, March 2021, https://www.aljazeera.com/news/2021/3/2/privacy-fears-as-indias-govt-schools-install-facial-recognition#:~:text=A%20personal%20data%20protection%20law%20is%20being%20drafted%20by%20Indian

AI Technologies and the Impact on Privacy and Free Association

States' use of AI-driven tools to monitor and surveil individuals via apps and social media platforms restricts the ability of people to freely associate and violates the rights to privacy.

The Special Rapporteur on the rights to freedom of peaceful assembly and of association describes the right to privacy as intimately related to the enjoyment of the right to association.[15] States' use of AI-based surveillance tools to monitor and limit association in online and offline spaces violates the right to privacy and the freedom of association. For example, the use of AI technology to surveil individuals via their cellphones is not only an invasion of privacy, but results in restrictions on the ability to freely associate. Such technology is utilized by states in a variety of ways. For example, China's use of AI-powered algorithms to conduct surveillance of communications in the WeChat app led to the arrest of individuals who were on their way to attend a poetry reading with friends.[16] Vietnam's monitoring of communications on Facebook using AI algorithms to search for language deemed critical of the government has led to many pages and groups being restricted or taken down.[17]

The use of AI technologies that invade individuals' privacy restrict their freedom of association. Individuals are less likely to join organizations and meetings due to fear of repercussions and those individuals that do lawfully exercise their right to freedom of association are subject to consistent violations of their right to privacy.

AI Technologies and the Impact on Privacy and Free Expression

States' use of AI-driven surveillance and tracking tools to monitor communications violates privacy and restricts the freedom of expression.

The right to privacy in communication encompasses the ability to ensure that communications remain private and secure.[18] "The right to privacy is often understood as an

%20legislators.&text=at%20the%20time.-,Facial%20recognition%20systems%20are%20often%20rolled%20out%20without%20a%20privacy,Centre%2C%20a%20digital%20rights%20nonprofit.; Reuters, *'Birds on the wire'? Concerns over Mexico cell phone surveillance,* June 2020, https://www.reuters.com/article/us-mexico-tech-rights-trfn-analysis/birds-on-the-wire-concerns-over-mexico-cell-phone-surveillance-idUSKBN23J2CC

[15] United Nations Human Rights Council, A/HRC/41/41, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule" May 17, 2019, para. 16.

[16] *See, e.g.,* NPR, *Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'*, Jan. 2021, https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta; WXPI, *Pittsburgh police used facial recognition technology during Black Lives Matter protests*, May 2021, https://www.wpxi.com/news/top-stories/pittsburgh-police-used-facial-recognition-technology-during-black-lives-matter-protests/VT52MGWM3VCDJINJSZPOO5NHKU/

[17] *See, e.g.,* Asia Times, *Facebook's self-defeating censorship in Vietnam,* Nov. 2020, https://asiatimes.com/2020/11/facebooks-self-defeating-censorship-in-vietnam/; Los Angeles Times, *Facebook touts free speech. In Vietnam, it's aiding in censorship*, Oct. 2020, https://www.latimes.com/world-nation/story/2020-10-22/facebook-censorship-suppress-dissent-vietnam; Digital Information World, *Private Facebook Groups, You Are Being Watched!* Aug. 2019, https://www.digitalinformationworld.com/2019/08/private-facebook-groups-you-are-being.html

[18] United Nations Human Rights Council, A/HRC/23/40, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" April 17, 2013, para. 23.

essential requirement for the realization of the right to freedom of expression," and "undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas."[19] The use of AI technologies by states to monitor and surveil the personal communications of individuals violates their right to privacy, as well as their right to free expression. For example, the Chinese tech company iFlytek uses voice recognition software to provide real-time language translation—as well as surveillance of individuals' cellphone conversations;[20] the company's software was used in the persecution of Uighur Muslims, resulting in iFlytek being put on a U.S. trade blacklist.[21] The use of voice recognition technology by the National Security Agency (NSA) in the US is well-established, and has raised concerns over the use of the technology, including the tracking of journalists and identifying whistle-blowers.[22] The potential uses of speech recognition technology to target activists and minorities are made even more worrying by the fact that these technologies have significant racial disparities; five leading speech-to-text services were found to have a 35% error rate for black speakers as compared to a 19% rate for white speakers.[23] In addition to violating the right to privacy and free expression of individual cellphone users, the use of such technology also creates a broader fear of violations of privacy in communications, and thereby has a wider chilling effect on free expression.

Conclusion

The use of AI technologies is inextricably linked to the right to privacy, and consequentially, to civic freedoms, including the freedoms of assembly, association, and expression. The use of AI technologies has grown exponentially in recent years, but most people have no idea how their governments use AI systems or for what purposes. This lack of awareness stems from a dearth of regulatory approaches governing AI. Ironically, the privacy surrounding governmental use of AI directly leads to increased privacy violations of individuals.

In order for the use of AI technologies to be aligned with international human rights standards, there must be awareness on the part of the population on the ways in which AI systems are being utilized, including the ability for individuals to opt out of such use. Furthermore, there must be meaningful public participation in the development of laws and regulations around the development and deployment of AI systems, which requires accountability and transparency, and openness and availability of information.[24] Regulations must also adhere to international human rights standards and ensure that uses of AI are legitimate and narrowly tailored.

---

[19] *Id.*

[20] Wired, *How a Chinese AI Giant Made Chatting—and Surveillance—Easy*, May 2020, https://www.wired.com/story/iflytek-china-ai-giant-voice-chatting-surveillance/

[21] Business Insider, *These Chinese firms were blacklisted for Uighur oppression. Now they want to sell COVID-19 surveillance tools to the West*, June 2020, https://www.businessinsider.com/blacklisted-chinese-firms-uighur-oppression-covid-19-surveillance-tech-2020-6

[22] *Id.*

[23] Stanford Computational Policy Lab, *The Race Gap in Speech Recognition Technology*, https://fairspeech.stanford.edu/

[24] United Nations Office of the High Commissioner for Human Rights, *Guidelines for States on the effective implementation of the right to participate in public affairs,* para 23, Retrieved from: https://www.ohchr.org/Documents/Issues/PublicAffairs/GuidelinesRightParticipatePublicAffairs_web.pdf

Contact Information

For further information or in case of questions, please contact Zach Lampell, ICNL Senior Legal Advisor – Digital Rights, at zlampell@icnl.org.