Privacy and Artificial Intelligence: GNI Submission to Thematic Report on "the Right to privacy in the Digital Age" from UN Human Rights

The Global Network Initiative (GNI) welcomes this opportunity to provide input to UN Human Rights on the preparation of the thematic report on artificial intelligence and the right to privacy, as requested in Human Rights Council resolution 42/15 on "The right to privacy in the digital age," and informed by the corresponding 27–28 May 2020 expert seminar.[1]

An increasing range of digital products and services rely on AI technologies. The COVID pandemic has underscored the extent to which these technologies now impact an incredibly wide range of human activities, and brings into sharp focus their political, social, economic, and public health implications. It is therefore opportune that this report will focus on the potential for the use of AI to help facilitate the promotion and protection of the right to privacy, as well as the challenges the use of AI poses to the effective exercise of privacy and other human rights.

GNI is a multistakeholder group of academic organizations and individuals, civil society organizations, information and communications technology (ICT) companies, and investors collaborating to forge a common approach to freedom of expression and privacy in the ICT sector. Members share a commitment to the GNI Principles, which provide high-level guidance to the ICT industry on how to respect, protect, and advance user rights to freedom of expression and privacy, including when faced with government demands for censorship and disclosure of user's personal information. The corresponding GNI Implementation Guidelines offer more detailed guidance for companies in putting the framework into practice and provide a basis for multistakeholder collaboration across GNI's four constituencies.[2]

GNI strives to share lessons from its unique experience with building trust and understanding among diverse stakeholders, as well as the considered, consensus views of our expanding membership. GNI regularly provides input to governmental, multilateral, and multistakeholder processes, including on the important work of UN Human Rights on privacy in the digital age.[3]

[1] https://www.ohchr.org/EN/Issues/DigitalAge/Pages/SeminarArtificialIntelligence.aspx

[2] See the full set of GNI members' core commitments here: https://globalnetworkinitiative.org/core-commitments-2/

[3] https://globalnetworkinitiative.org/wp-content/uploads/2018/05/GNI-Input-OHCHR-Privacy-Report.pdf ; https://www.ohchr.org/Documents/Issues/Privacy/GlobalNetworkInitiative.pdf

Risks and Opportunities for Privacy and Other Human Rights

As stated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and reiterated in the GNI Principles, everyone should be free from illegal or arbitrary interference with the right to privacy and should have the right to the protection of the law against such interference or attacks. The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws or standards and the rule of law and be necessary and proportionate for the relevant purpose.

Over time, intelligence organizations and law enforcement agencies have expanded the tactics and capabilities they use to obtain access to private information , including through artificial intelligence-enabled tools.[4] The use of tools that rely upon biometric data — i.e., the recognition of human features — warrants particular scrutiny. Without sufficient safeguards, the use of biometric data by public authorities can result in deep intrusion into private lives of individuals, limit individuals' freedom of association, and have discriminatory impacts.[5] As Fionnuala Ní Aoláin, UN Special Rapporteur on the protection and promotion of human rights while countering terrorism, noted in the 27–28 May 2020 expert seminar, the growing adoption of these tools in areas like border management, law enforcement, and intelligence gathering has not necessarily been accompanied by corresponding human rights guidance.[6]

Another potential application for AI technologies is for exceptional access to user data, including the sorting, analysis, and/or interception of data flows, including web traffic and digital communications. In cases where AI technologies are used to facilitate access to data streams without the knowledge of service providers, these forms of surveillance could constitute "direct access" arrangements.[7] By taking service providers "out of the loop," direct access arrangements remove an important potential source of scrutiny, transparency, and accountability for government surveillance activities. Removing this potential safeguard increases the likelihood that direct access arrangements will result in arbitrary or unlawful interference with the privacy rights of the users of such services. These arrangements differ from traditional lawful interception mechanisms in that they are often not subject to the same

---

[4] For more on the increased adoption of smart cities, facial recognition systems, and smart policing tools, see "The Global Expansion of AI Surveillance," Steven Feldstein, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

[5] https://cdt.org/insights/cdtes-response-to-the-council-of-europes-ad-hoc-committee-on-artificial-intelligence-cahai-consultation-on-a-legal-framework-on-ai/; https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx, recital 12

[6] https://www.ohchr.org/Documents/Issues/DigitalAge/ExpertSeminarReport-Right-Privacy.pdf, page 11

[7] GNI statement, "Defining Direct Access," forthcoming. Will be available at https://globalnetworkinitiative.org/policy-issues/surveillance/.

legal procedures that mitigate and provide oversight of law enforcement requests, critical details about their implementation are often confidential, and they tend to target data in bulk.

Finally, some governments' approaches to addressing digital harms in their respective jurisdictions raise significant freedom of expression and privacy concerns, as we detail in our "Content Regulation and Human Rights" policy brief.[8] Of particular concern are laws and regulations requiring or otherwise strongly incentivizing the use of automated tools or proactive measures to identify illegal or otherwise harmful content. Some of these efforts would go further by requiring service providers to proactively turn accounts and user information associated with such activity over to authorities. Such tools not only raise risks of invasion of privacy, but also may result in over-removal and increase risks of self-censorship, potentially chilling freedom of expression.[9] As former UN special rapporteurs on freedom of opinion and expression have noted, "privacy and expression are intertwined in the digital age, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression."[10] Other content regulation efforts would require service providers to track and/or trace all individual users' communications and activity, so that it can be attributed. Mandating invasive steps along these lines will make it difficult or impossible for services and users to deploy privacy and security-preserving features, such as end-to-end encryption.

Recommended Safeguards

Whether governments are deploying AI-enabled technology directly, or requiring or incentivizing its use by other actors, it is critical that they continue to ensure that the development, design, and deployment of such technology is governed by adequate transparency and accountability. Without sufficient and appropriate governance frameworks that allow for independent scrutiny, risk identification and mitigation, public awareness and education, individual choice/ability to opt-out, and appropriate remedy, public trust will be undermined and the potential benefits of AI-enabled technologies will be jeopardized.

Meanwhile, companies must also ensure that their development and use of AI-enabled technology, including its sale to public sector actors, is consistent with their responsibility to respect human rights, including the right to privacy. GNI's multistakeholder framework offers a model for the ICT sector to ensure respect for privacy and freedom of expression in their products, services, and operations, including those utilizing AI.

---

[8] https://globalnetworkinitiative.org/content-regulation-policy-brief/

[9] See "Mixed Messages? The Limits of Automated Social Media Content Analysis" by Emma Llansó and Natasha Duarte https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/

[10] A/HRC/41/35, para. 24; A/HRC/29/32; and A/HRC/23/40, para. 24)

The Implementation Guidelines encourage companies to consider human rights, including privacy, as part of their longer-term strategic planning and investment decisions. For instance, participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.

Consistent with the UN Guiding Principles on Business and Human Rights, and international human rights standards, the Implementation Guidelines also clarify that participating companies will carry out human rights due diligence (HRDD) to identify, prevent, evaluate, mitigate, and account for risks to the freedom of expression and privacy rights that are implicated by the company's products, services, activities, and operations. These processes should be ongoing, and when they identify circumstances when freedom of expression and privacy may be jeopardized or advanced, participating companies will employ human rights impact assessments (HRIA) and develop effective risk mitigation strategies as appropriate. GNI remains eager to continue engaging with experts working on further guidance and good practices for HRDD and HRIA as applicable to artificial intelligence, including with UN Human Rights.[11]

As artificial intelligence products increasingly rely on large and detailed sets of sensitive personal data and governments expand their tactics and capabilities for accessing this data, the Implementation Guidelines ask companies to proactively engage with governments to ensure that international laws and standards on freedom of expression and privacy are upheld. Participating companies encourage governments to be specific, transparent, and consistent in the demands, laws, and regulations that impact the right to privacy, including demands that are issued regarding privacy in communications. The Guidelines advise participating companies to adopt policies and procedures that set out how the company will assess and respond to government demands for restriction to communications or access to content, or disclosure of personal information. These policies also address situations where governments may make demands through proxies and other third parties to evade domestic legal procedure.

Participating companies are also expected to be transparent about government access to personal information and communications. The Guidelines encourage participating companies to disclose, to the extent allowed under the law, what laws and policies compel them to provide personal information to government authorities, what personal information the participating companies collect, and the company's policies and procedures for responding to government demands. One example of GNI's collective effort to increase transparency about pertinent legal powers is the GNI Country Legal Frameworks (CLFR).[12] The CLFR is a detailed set

[11] See focus area 2 of the UN Human Rights "B-Tech" project in particular: https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx

[12] Available at https://clfr.globalnetworkinitiative.org/

of resources examining governments' legal authorities to intercept communications, obtain access to communications data, or restrict the content of communications in more than 50 countries.

Companies participating in GNI are independently assessed every two years on their progress in implementing the GNI Principles.[13] The purpose of the assessment is to enable the GNI Board to determine whether each member company is "making good faith efforts to implement the GNI principles with improvement over time." Independent third parties are accredited and must meet strict independence and competency criteria, and produce assessment reports reviewed by the GNI Board. The assessment process is confidential by nature and contributes to trust built among members that underpins our shared learning function. This shared learning allows GNI to harness members' collective intellectual and practical experience and the capabilities of our diverse membership to bring unparalleled resources to bear on emerging and challenging issues, including the application of artificial intelligence technologies.

Legal and Regulatory Considerations

The GNI Principles state that individually and collectively, participants will engage governments and international institutions to promote the rule of law and the adoption of laws, policies and practices that protect, respect and fulfill freedom of expression and privacy. The broad scope of potential applications for artificial intelligence, as well as the varying degrees to which they require the collection of personal data, makes a one-size-fits-all approach to the regulation of artificial intelligence difficult. We support the risk-based approach taken by various national and multilateral initiatives considering legal frameworks for AI, which target the uses of artificial intelligence that offer the most salient risks and tailor requirements accordingly. The application of artificial intelligence by public actors, including law enforcement, deserves at least as much, if not more, scrutiny as commercial applications, and any requirements for privacy risk assessments or HRDD or HRIA should apply equally to commercial and public uses.[14] The international human rights framework should underpin any efforts to regulate AI, providing an important baseline from which to analyze risks and opportunities effectively, as well as to ensure that myriad efforts at national, regional, and international levels to regulate AI are in sync.

[13] Read more about the independent GNI company assessment process here: https://globalnetworkinitiative.org/company-assessments/

[14] In the EU proposal for a regulation on artificial intelligence, some groups have praised the restrictions on the application of biometric data for law enforcement purposes while criticizing exceptions to requirements for AI technologies when used for national security purposes https://edri.org/our-work/eus-ai-proposal-must-go-further-to-prevent-surveillance-and-discrimination/

As AI technologies are often reliant on personal data, and the ease of access to data storage increases, there are important principles that should underpin any laws or policies enabling governments to lawfully request and access electronic evidence. They should be developed with multistakeholder input, include appropriate transparency measures, require independent authorization and oversight of government access, and ensure accountability. To the greatest extent possible, these laws should be publicly available, and should enable companies to be transparent about their application, including about statistics for government requests. They should avoid mandates to companies or other third parties to store data that they would otherwise not retain in order to facilitate government access. Finally, with the growth in the government acquisition of private technologies that can facilitate AI-enabled surveillance,[15] governments should also consider strengthening export controls for such technologies in countries with repressive track records and/or weak rule of law, in line with UN Guiding Principles for Business and Human Rights.

Conclusion

There has been much discussion about the potential for artificial intelligence technologies to provide immense economic and social benefits, as well as our growing reliance on digital products and services during the pandemic. With the growing role of AI in our day-to-day lives, GNI recognizes the importance of ensuring that AI technologies contribute to the protection and promotion of the rights to privacy, and we appreciate UN Human Rights focus on this issue. As we have noted throughout this submission, we feel the GNI Principles can serve as a model to guide ICT companies to provide and utilize AI technologies in rights-respecting ways. In addition, the Principles and corresponding Implementation Guidelines can guide companies and other stakeholders in engaging with regulators and lawmakers to ensure that any corresponding restrictions on privacy and freedom of expression resulting from government use or regulation of AI are necessary and proportionate to achieve a legitimate purpose. We stand ready to continue engagement with UN Human Rights, member states, and other UN bodies working to address privacy in the digital age.

[15] A/HRC/41/35, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736