Check against delivery

Statement of Dr. Ana Brian Nougrères

SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY

61st session of the Human Rights Council

Agenda Item 3

11 March 2026

Geneva

Distinguished delegates, members of the Human Rights Council, and representatives of civil society,

It is an honour to present my latest thematic report, A/HRC/61/48, on the international collection of personal data. This report serves as a vital supplement to my 2024 submission to the General Assembly, where I proposed updating the UN 1990 Guiding Principles for computerized data files.

Let me start by saying that, for decades, our legal frameworks have focused on international data transfers. We built rules based on the "principle of continuity", ensuring that when a sender in Country A exports data to Country B, the protection "travels" with it. In these scenarios, local authorities can control the sender. However, the digital landscape has shifted dramatically.

We are now witnessing a massive scale of international collection. This occurs when a collector in Country B extracts data directly from individuals in Country A without any physical presence in that territory. Unlike transfers, there is no data sender for local authorities to regulate at the source.

Every person with an internet connection is now a potential international collector. International collectors often argue that because they are not domiciled in the data subject's country, local laws do not apply. They claim immunity from investigation or punishment. But as my report highlights, physical absence does not mean a lack of impact.

Through tools like cookies and mobile applications, entities establish a "technological presence". These tools track browsing habits, search histories, and even location data from millions of citizens without the collector ever setting foot in their country.

This has been confirmed by authorities in countries like Colombia, where it was found that major global platforms process the data of millions, including children, through these "invisible" mechanisms.

The current global situation is fragmented. While some regions, such as the European Union through the GDPR, have introduced extraterritorial scope, these rules often only apply to specific situations like the offering of goods or monitoring of behavior.

In many other parts of the world, there are no general regulations on personal data processing at all. This creates "data havens", jurisdictions where the protection of rights is weak or non-existent, attracting those who wish to evade privacy laws.

If we rely solely on a strict principle of territoriality, we allow the internet to become a zone of impunity. Unilateral efforts are no longer enough; global problems require global solutions.

I respectfully urge Member States to take two decisive steps:

First, we must draft a legally binding international treaty that comprehensively addresses the challenges of international data collection and ensures individuals' rights are protected regardless of where the collector is domiciled.

Second, we must modify the scope of local regulations to ensure they cover extraterritorial situations, preventing companies from using a lack of physical headquarters as a shield against accountability.

We must not "normalize" a situation where human rights are ignored in cyberspace. It is time to ensure that the law is as borderless as the data it seeks to protect.

We stand at a defining crossroads where the digital frontier must finally meet the boundaries of human dignity. The international collection of personal data is not merely a technical or jurisdictional challenge; it is a test of our collective resolve to ensure that the progress of the 21st century does not come at the cost of our fundamental rights.

We must firmly reject the notion that because data collectors lack a physical presence in a territory, they are beyond the reach of justice or accountability.

Instead, let us envision a world where every individual, regardless of their nationality or location, can navigate the digital sphere with the absolute certainty that their privacy is not a commodity for extraction, but a sacred right protected by the force of law.

This transition requires us to acknowledge that while technology is borderless, the protection of the person must be equally pervasive, transforming the "technological presence" of collectors into a platform for responsibility rather than a shield for impunity.

Our mission requires us to look beyond our own borders and recognize that in this interconnected age, the vulnerability of one citizen is the vulnerability of all.

As my report emphasizes, unilateral and isolated efforts by individual countries are simply no longer sufficient to address global phenomena like the "data havens" that threaten to undermine our shared human rights standards.

We must foster a spirit of unprecedented international cooperation, where States, data protection authorities, and civil society work in unison to ensure that protection truly "travels" with the data.

By closing the regulatory gaps that encourage jurisdictional evasion, we are not just protecting information; we are safeguarding the very fabric of our democratic societies and the personal autonomy of our citizens.

Let this session be remembered as the moment we chose to replace legal uncertainty with a robust framework of mutual assistance and a shared, unwavering commitment to the universal right to privacy.

Finally, let us act with the urgency that this era demands for the millions of people whose lives are continuously impacted by the invisible hands of international data collectors.

We have the historic opportunity to lead the way toward a legally binding international treaty that finally bridges the gap between our outdated laws and our current digital reality.

We owe this especially to the children and adolescents who are growing up in a world where their every interaction is being harvested and analyzed. Our legacy should not be one of silence in the face of technological exploitation, but one of courage in drafting the rules that will define the digital century.

Privacy is the foundation upon which all other freedoms are built; by securing it today through modern international collection regulations, we are securing a future where technology serves humanity, and where the dignity of the individual remains the north star of our global community.

Country Visits

I conducted my fourth official country visit to **Mongolia** from 8 to 14 April 2025.
My objective was to evaluate the right to privacy in Mongolia and support the “Public Inquiry on Human Rights and Technology (2024-2025) conducted by the National Human

Rights Commission on issues of common interest, including the personal data protection system, cybersecurity, surveillance, oversight mechanisms and remedies, new and emerging technologies and privacy concerns of vulnerable groups.

Mongolia implemented the Protection of Personal Data Protection law in 2022, which provided a much-needed comprehensive update to the legal framework. The greatest challenge is not in the adequacy of the laws but *implementation* of an accessible complaint mechanism that provides transparency and accountability.

I noted several challenges but a key element, the *political will*, is present. However, there needs to be a corresponding shift in the mindset of its citizens so *they* view the right to privacy as a fundamental human right. The concept of privacy, in particular informed consent, is not well understood by its citizens, both in the city (where over half the population resides) and even more in rural areas.

The Government is invested in emerging technologies to elevate its economic and social development and I observed a strong commitment to privacy - a key element to ensure a human rights approach. Additional measures are needed to balance innovation, security and privacy by strengthening and coordinating oversight powers.

The launch of E-Mongolia is a positive initiative that has delivered benefits and increased awareness of privacy and security issues for some of the population, but further outreach is needed to deepen inclusion, build digital skills and strengthen institutional trust.

My report contains numerous recommendations aimed at specific groups, for example:

Develop robust security measures and equitable access to, digitalization through the E-Mongolia system for *all* essential government services, particularly in the health sector and social protection services, to ensure that vulnerable groups who most depend on these services can access them in a manner that protects their right to privacy.

Address underreporting of tech-facilitated gender based violence by developing methodologies to investigate technology-facilitated crimes, to identify, secure, and evaluate digital evidence, and train law enforcement.

Strengthen policies, laws and regulations to incorporate specific strategies to reduce the risks of cyberbullying, online exploitation and abuse of children and young people.

As a priority, I urge the Government to create an independent Data Protection Authority with a robust oversight mechanism to conduct investigations, issue guidelines *and* binding remedial powers that can be appealed to the courts. This will be particularly challenging as it will require significant financial resources to be effective.

Thank you for your attention.

****