Joint NGO letter to the newly appointed UN Special Rapporteur on the right to privacy

3 July 2015

Dear Mr. Cannataci,

We represent twenty-three organisations, from across the globe, dedicated to promoting the rights to privacy and free expression.

We congratulate you on your appointment. As members of civil society, we believe that as Special Rapporteur you can have an extraordinary impact on States' and companies' respect for, and protection of, the right to privacy.

Many of us live and work in the Global South, where privacy is key to creating a healthy environment for citizen engagement, and to protecting individuals from discrimination and social marginalisation. However, the right to privacy is threatened by corporate and political interests, resulting in individuals' privacy often being set aside in favour of development and security priorities. As a consequence, privacy is not always given sufficient recognition as a fundamental human right, nor has it received the necessary attention as a public policy issue, leading to many violations of this right in many contexts.

Further, violations of the right to privacy are committed not only by our own governments, but by the governments of other countries, which have the technical capacity to intercept,

access, store and analyse private communications extraterritorially or as such communications travel across or are stored in their territories.

In recent years, we have seen technological developments that, when used by powerful companies and unaccountable law enforcement and intelligence services, unlawfully interfere with everyone's privacy. Technological advancements in processing personal data (including the ever-increasing power to intercept, access, collect, store and analyse data; centralised DNA and biometric databases; and more sophisticated algorithms able to de-anonymise data) are outpacing existing, out-of-date legal protections. Meanwhile, the emergence of a fast-expanding global surveillance industry, exporting products and services to governments across the world with few controls, is enabling government agencies to use such technology to interfere with the right to privacy, including by conducting mass surveillance.

Technological developments are coupled with a global discourse on security and counter-terrorism that treats the privacy of individuals as an impediment to the pursuit of vaguely or broadly defined national security aims, wrongly pitching privacy against security. This discourse has led to the adoption of national legislation that grants intelligence services extended powers with little oversight, particularly under the notion of addressing cyber crime, cyberwarfare and cyber terrorism.

This is of particular concern as countries traditionally associated with rule of law and respect of human rights have been at the forefront of the attempts to unlawfully restrict the enjoyment of the right to privacy in the name of national security and counter-terrorism, sometimes introducing laws to post facto legitimise their practices. This is creating a vicious cycle, leading to a race to the bottom, with countries seeking to justify their repressive laws and policies by pointing at recent developments in other countries, without due regard to the applicable, legally-binding international human rights standards.

Today, we face many serious threats to privacy in our countries. They include intelligence structures with expansive mandates and wide ranging powers to snoop on the everyday activities of ordinary citizens without effective oversight; criminalisation or other unlawful limitations on anonymity and access to encryption technologies; and the proliferation of identity systems that use technology to catalogue, control and exclude vulnerable groups.

Secrecy surrounding the actions (or even the legal framework) of state security and intelligence agencies remains pervasive, together with weak laws that protect privacy and regulate their activities, and unregulated and opaque acquisition of surveillance technologies. In fact, civil society organisations even face threats when documenting violations of the right to privacy, and when researching state policies and practices.

State surveillance and misuse of data take many forms in our countries, such as mass interception of communications; indiscriminate data retention policies; locational surveillance, via CCTV, GPS and similar technology; mandatory registration of SIM cards, compulsory IDs, and biometric systems. Personal information so gathered are then used to target opposition politicians (including for blackmailing), union workers, journalists and human rights defenders. Hacking, malware and other means of compromising the security of communication systems are likewise pursued with increasing success by security and intelligence agencies, sometimes using the same criminal techniques that they profess to combat.

We also experience societal and structural impediments to the enjoyment of the right to privacy. These impediments take the form of a general lack of awareness about privacy and the harms that ensue when it is not protected effectively. In some countries, this is compounded by a prevailing patriarchic and misogynist attitude which fuels privacy violations, especially against women and girls. Government failure to support the functioning of existing privacy laws, including the provision of necessary resources to the bodies mandated to implement them (such as privacy or data protection authorities) is further exacerbated by the lack of specific training for the judiciary and the broader legal community on both the legal and technical aspects of the right to privacy.

That is why the appointment of a Special Rapporteur on the right to privacy is so essential. We very much hope that you can provide expert analysis of and guidance on the human rights framework applicable to the right to privacy. We would also like to see you tackle key privacy challenges such as defining the scope of the right to privacy, in particular as it applies to new technologies; identifying the judicial and other oversight mechanisms necessary to supervise those actors involved in the surveillance of communications; responding to the threats human rights defenders and other actors face from the use of surveillance; and addressing the lack of understanding of the right to privacy.

We would like to recommend that you develop your analysis and recommendations in collaboration and coordination with other existing independent human rights experts, whose mandates touch upon common issues and challenges. We would also like to encourage you to consider, from the onset of your tenure, participating in relevant international and regional gatherings, such as the international conference of data protection and privacy commissioners, to establish contacts and develop relationships with relevant experts.

We would welcome the opportunity to discuss these and other issues with you in person, and are available to provide support and expertise as you require.

Yours faithfully,

1. **Africa Platform for Social Protection, Kenya**
2. **Asociación por los Derechos Civiles, Argentina**
3. **Association des droits numeriques, Morocco**
4. **Bytes for All, Pakistan**
5. **Centre for Cyber Law Studies, Indonesia**
6. **Center for Internet and Society, India**
7. **Coding Rights, Brazil**
8. **Dejusticia, Colombia**
9. **Derechos Digitales, Chile**
10. **Digital Rights Foundation, Pakistan**
11. **Foundation for Media Alternatives, Philippines**
12. **Fundación Karisma, Colombia**
13. **Institute for Policy Research and Advocacy (ELSAM), Indonesia**
14. **The Law and Technology Centre, Faculty of Law, the University of Hong Kong, Special Administrative Region of the People's Republic of China**
15. **Kelin, Kenya**
16. **Jonction, Senegal**
17. **Nawaat, Tunisia**
18. **Privacy International, United Kingdom**
19. **R3D, Mexico**
20. **Right2Know, South Africa**
21. **Voice, Bangladesh**
22. **Unwanted Witness, Uganda**
23. **Zimbabwe Human Rights NGOs Forum, Zimbabwe**