Amnesty International and Privacy International's seven-point plan for protecting human rights in the digital age

Legal and policy reform

1. National laws should be reformed to ensure that they comply with international human rights law and standards, including by not allowing for indiscriminate mass surveillance. Key principles that must be upheld include:
a. Ensuring that surveillance of communications only happens when it is targeted, based on sufficient evidence of wrongdoing, and authorised by a strictly independent authority, such as a judge;
b. Ensuring there is transparent and independent parliamentary and judicial oversight of surveillance powers;
c. Making rules and policies about surveillance publicly available, including how governments are sharing information with other states;
d. Ensuring equal privacy protections apply for nationals and non-nationals, those within the territory of the state, and those outside it.
e. Intelligence sharing should be strictly regulated and conducted in a manner compliant with states' human rights obligations;

2. Governments should not make encryption and anonimization technologies, or their use, illegal;

3. Whistleblowers, including those working on national security issues, should be afforded strong legal protection from any form of retaliation, including by way of prosecution, for having disclosed public interest information such as on human rights violations.

Corporate due diligence

In line with companies' responsibility to respect human rights:

4. Companies that own and/or operate telecommunications or internet infrastructure, including undersea telecommunications cables, and internet companies, must ensure that access to data is permitted only when it conforms to international law and standards on human rights, including by taking legal action to challenge government requests that seek bulk/wholesale access to communications traffic;

5. Major internet and telecommunications companies should lead the way in using strong encryption and other privacy technologies, including through implementing end-to-end encryption by default, where possible;

6. Internet service providers, telecommunications companies and internet companies should clearly inform users about legal requirements that they have to comply with, particularly in relation to handing over user information or content.

International standards

7. Further explore and develop means and measures needed to ensure better implementation of the international human rights standards applicable to communications surveillance, building on efforts towards identifying relevant elements that have started in the past two years, including reports by the UN Special Rapporteur on Freedom of Expression, the UN High Commissioner of Human Rights the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, as well as civil society initiatives such as the Necessary and Proportionate Principles.