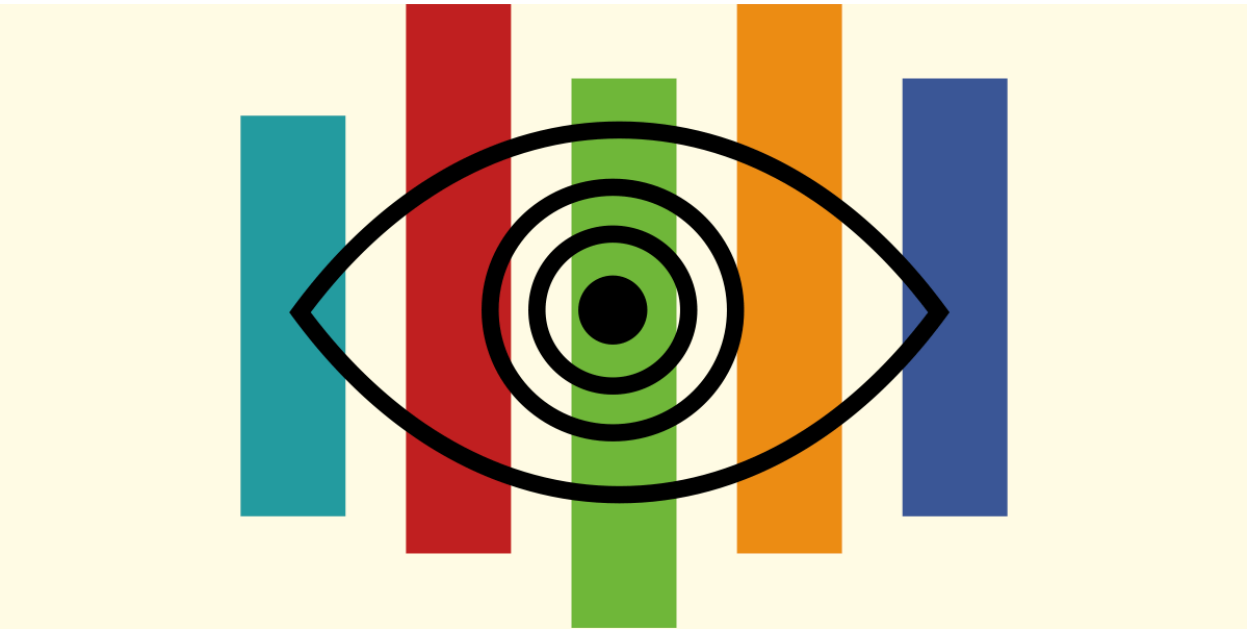
Necessary and Proportionate



International human rights law already protects privacy, freedom of expression, and the rule of law. But as governments develop more technologically sophisticated ways to surveil more communications of more innocent people, the application of that law has lagged behind. The 13 Principles outline how modern communications surveillance can be consistent with human rights.

Who Has Signed?

- More than 400 organizations supporting human rights, access to knowledge, the environment, women's rights, free expression, and a free press from around the world.
- Experts, academics, security researchers, political parties, and elected officials from more than 20 countries.
- Thousands of individuals throughout the world.

How are the principles being used?

The 13 Principles now serve as a model for reform of surveillance law and policy around the world. Policymakers, elected officials, companies, NGOs and activists use them to advocate for a minimal universal standard for government and law enforcement surveillance practices. They are used as an established benchmark for measuring whether a State's surveillance practices comply with human rights law.

And where surveillance law does not conform to the Principles, their language is used to hold government accountable, and push toward effective oversight and transparency, enact safeguards, and limit unchecked surveillance.

EFF

Summary of the 13 Necessary and Proportionate Principles

1. **Legality:** Limits on the right to privacy must be set out clearly and precisely in laws and should be regularly reviewed to make sure privacy protections keep up with rapid technological changes.
2. **Legitimate Aim:** Communications surveillance should only be permitted in pursuit of the most important state objectives.
3. **Necessity:** The State has the obligation to prove that its communications surveillance activities are necessary to achieving a legitimate objective.
4. **Adequacy:** A communications surveillance mechanism must be effective in achieving its legitimate objective.
5. **Proportionality:** Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Proportionate communications surveillance will typically require prior authorization from a competent judicial authority.
6. **Competent Judicial Authority:** Determinations related to communications surveillance must be made by a judicial authority that is impartial and independent.
7. **Due Process:** Any interference with human rights is governed by lawful procedures which are publicly available and applied consistently in a fair and public hearing.
8. **User Notification:** Individuals should be notified of a decision authorizing surveillance of their communications. Except when a competent judicial authority finds that notice will harm an investigation, individuals should be provided an opportunity to challenge such surveillance before it occurs.
9. **Transparency:** The government has an obligation to make enough information publicly available so that the general public can understand the scope and nature of its surveillance activities. The government should not generally prevent service providers from publishing details on the scope and nature of their own surveillance-related dealings with State.
10. **Public Oversight:** States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions.
11. **Integrity of Communications and Systems:** Service providers or hardware or software vendors should not be compelled to build surveillance capabilities or backdoors into their systems or to collect or retain information purely for surveillance purposes.
12. **Safeguards for International Cooperation:** On occasion, states may seek assistance from foreign service providers to conduct surveillance. This must be governed by clear and public agreements that ensure the most privacy-protective standard applicable is relied upon in each instance.
13. **Safeguards Against Illegitimate Access:** There should be civil and criminal penalties imposed on any party responsible for illegal electronic surveillance and those affected by surveillance must have access to legal mechanisms necessary for effective redress. Strong protection should also be afforded to whistleblowers.

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org