Guiding principles

- European Convention on Human Rights & Council of Europe data-protection rules apply to all personal data processing activities by all agencies, including national security and intelligence agencies
- Human rights obligations shall not be circumvented through ad hoc arrangements with private actors
- No states & none of their agencies should access data stored in another country without express consent of the other country or countries involved, unless there is a clear legal basis & access complies with Human Rights standards
- Jurisdiction
  - Need to limit the exercise of extra-territorial jurisdiction in relation to transnational cybercrimes
  - States should only exercise jurisdiction over foreign materials that are not illegal under international law if there is a nexus between the materials or the disseminator & the state taking action
- Cybercrime
  - All states parties to the Convention on Cybercrime must comply with their human rights obligations in anything they do or do not do under the Convention
  - States must ensure that their law enforcement agencies do not obtain data from servers & infrastructure in another country under informal arrangements
- Data protection
  - Ratify & implement Council of Europe Data-protection Convention No. 108
  - Strengthen Convention No. 108 to clarify & better enforce rules, especially in relation to digital world, surveillance for national security, & intelligence purposes
  - States must not resort to or impose mandatory retention of data by third parties
- Privacy
  - Strengthen Convention No. 108 to clarify & better enforce rules, especially in relation to digital world, surveillance for national security, & intelligence purposes
- National security activities
- Recommendations
  - Interfere with human rights only in cases that threaten the very fabric & basic institutions of a country
  - Interferences can occur only prior proof that the threat cannot be met by means of ordinary criminal law
  - Strengthen democratic oversight of national security & intelligence agencies
- Blocking & filtering
  - Restrictions on access to Internet content must be based on a strict & predictable legal framework with judicial oversight
  - Do not rely on or encourage private actors to carry out blocking outside this framework
- Concerns
  - States’ reliance on private-sector companies to circumvent their own human rights obligations
  - States with global influence on the Internet not complying with international Human Rights standards in their digital activities
  - Competing and conflicting laws on freedom of expression applying simultaneously
  - Blurred lines between law enforcement & national security activities & agencies in the digital environment

Respecting the rule of law on the Internet and in the wider digital environment

Image: Submarine cable map - courtesy of www.submarinecablemap.com