Digital Freedoms in International Law

Dr. Ian Brown and Prof. Douwe Korff
Sources of law

- International Covenant on Civil and Political Rights (1966), esp. §17-§19, §21, §22
- Interpretation by the UN Human Rights Committee, UN High Commissioner for Human Rights
- UN Special Rapporteurs
  - On Freedom of Opinion and Expression
  - On the promotion and protection of human rights and fundamental freedoms while countering terrorism
  - On human rights and transnational corporations
ICCPR signatories

Data: UN High Commissioner for Human Rights; Graphic: WikiMedia
“Terrorism clearly has a very real and direct impact on human rights, with devastating consequences for the enjoyment of the right to life, liberty and physical integrity of victims. In addition to these individual costs, terrorism can destabilize Governments, undermine civil society, jeopardize peace and security, and threaten social and economic development. All of these also have a real impact on the enjoyment of human rights.

“Security of the individual is a basic human right and the protection of individuals is, accordingly, a fundamental obligation of Government. States therefore have an obligation to ensure the human rights of their nationals and others by taking positive measures to protect them against the threat of terrorist acts and bringing the perpetrators of such acts to justice.”
Restrictions on rights must:

1. Be based on "law" - on published, clear and specific legal rules, the application of which is reasonably foreseeable;

2. Serve a legitimate aim in a democratic society - including law enforcement and protection of national security. Such limitations should not be abused for other ends, such as to protect a government from embarrassment or exposure of wrongdoing;

3. Be "necessary" and "proportionate" to that aim, and not impair the essence of the right;

4. Not involve discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, nationality, property, birth or other status;

5. Not confer excessive discretion on the relevant authorities;

6. Be subject to effective (judicial) safeguards and remedies.
"The framework comprises three core principles: the state duty to protect against human rights abuses by third parties, including business; the corporate responsibility to respect human rights; and the need for more effective access to remedies."

Companies faced with state demands that violate human rights have a duty to refuse to do so where they can, minimise the extent of any such cooperation, and help victims of any enforced cooperation.

GNI Principles and Implementation Guidelines already go a long way to operationalising the Guiding Principles.
Recommendations

• Greater sharing of knowledge on legal systems and experiences - to aid market entry and exit decisions, and assessments of legally binding requests for connection terminations, user data, and blocking

• Mechanisms for limiting use of products and services for serious human rights violations (contracts, dispute resolution, diplomatic support, technical measures)

• Careful planning of user data storage, requirement for legally binding requests, and renewed focus on (streamlined and speedier) MLATs for remote access, with backing in domestic law and contracts

• More transparency (states and companies), with aggregated reporting of user data access and blocking
“82 countries have signed and/or ratified a binding cybercrime instrument...multilateral cybercrime instruments have influenced national laws indirectly, through use as a model by non-States parties, or via the influence of legislation of States parties on other countries.” (p.xix, UNODC Comprehensive Study on Cybercrime, 2013)
Extra-territorial evidence

Key issue for further international cooperation (p.xxv, UNODC Comprehensive Study on Cybercrime, 2013)
CoE CC §32: “A Party may, without the authorisation of another Party...access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.”