

HMDC Presents... SPECPOL: Sample Draft Resolution

HMDC Presents... Sample Draft Resolution: SPECPOL: Corporate Surveillance, Accountability and Privacy

THIS IS A MODEL TO LEARN FROM, NOT TO COPY. We study this sample at home to learn the shape of a resolution and the kind of ideas that belong in it. In committee, we write every clause live, in our own words, with our bloc.

HOW A RESOLUTION IS BUILT

A resolution has two kinds of clauses. **Preambulatory clauses** come first: they explain why the committee is acting by recalling past resolutions, treaties and facts. Each one begins with an *italic* opening word or phrase, such as *Recalling* or *Deeply concerned*, and ends with a comma.

Operative clauses come second: they say what the committee will actually do. Each one is numbered and begins with a **bold** (or underlined) verb, such as **Calls upon** or **Requests**. Each ends with a semicolon, except the final clause, which ends with a period. SPECPOL is a General Assembly committee, so it cannot pass binding law or order companies to act. That is why our operative verbs *recommend*, *urge*, *request* and *encourage* instead of commanding.

THE SAMPLE DRAFT RESOLUTION

Committee: Special Political and Decolonization Committee (SPECPOL) **Topic:** Corporate Surveillance, Accountability and Privacy **Sponsors:** The Kingdom of the Netherlands, the Kingdom of Norway, the Oriental Republic of Uruguay, the Republic of Moldova **Signatories:** [signatories]

The Special Political and Decolonization Committee,

Recalling Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966), which protect every person from arbitrary or unlawful interference with privacy and correspondence,

Reaffirming General Assembly resolution 68/167 (2013), the first resolution on the right to privacy in the digital age, and resolution 79/175 (2024), which expresses deep concern about tools developed by the private surveillance industry to hack devices and collect data on journalists and human rights defenders,

Guided by the Guiding Principles on Business and Human Rights, endorsed by Human Rights Council resolution 17/4 (2011), which state that states must protect, companies must respect, and victims must have access to remedy,

Deeply concerned that at least 65 governments have acquired commercial spyware and that more than 500 companies reportedly develop and sell surveillance tools to governments (United Nations Human Rights Office, August 4, 2022),

Noting with regret that the Wassenaar Arrangement was built to reduce military threats and lacks guidelines or enforcement on human rights (UN Special Rapporteur on Freedom of Expression, May 28, 2019),

Noting with concern that only 137 of 194 countries have legislation to protect data and privacy (UN Trade and Development, Last Accessed: October 2026),

Welcoming the Global Digital Compact, adopted in resolution 79/1 (2024), in which world leaders committed to ensure that laws on surveillance and encryption follow international law and called on the UN system to help developing countries build capacity for data governance,

1. **Calls upon** all Member States to add a human rights assessment of the receiving country to every export licence for surveillance technology, and to deny a licence where the technology is likely to be used against journalists, activists or political opponents;
 2. **Recommends** that Member States permit the use of spyware by their own authorities only:
 - a. With prior approval from an independent judge;
 - b. For a specific serious crime or threat, as a last resort;
 - c. For a fixed and limited period of time;
 - d. With notice to the person targeted once the investigation has ended;
 3. **Encourages** Member States to adopt purchasing rules that bar their own agencies from using commercial spyware that poses serious security risks or has been misused by foreign governments;
 4. **Urges** all businesses that collect and process personal data, including data brokers, to:
 - a. Inform users clearly about what data is collected and why;
 - b. Collect data only with consent or another legal basis;
 - c. Allow people to access, correct and delete their own data;
 - d. Notify relevant parties when misuse of their products is detected;
 5. **Requests** the Office of the United Nations High Commissioner for Human Rights, through its B-Tech Project, to prepare guidance for companies that sell surveillance technology on applying the Guiding Principles on Business and Human Rights;
 6. **Establishes** a voluntary Data Protection Capacity Fund, financed by voluntary contributions from Member States so that it does not depend on the strained UN regular budget, to help countries without data protection laws write those laws and train independent authorities to enforce them;
 7. **Encourages** Member States, including states outside Europe, to consider joining the modernised Council of Europe Convention 108+, which updates Convention 108, the first legally binding international treaty on data protection;
 8. **Invites** Member States to join the Pall Mall Process and to support its voluntary Code of Practice for States, built on accountability, precision, oversight and transparency;
 9. **Calls upon** Member States not to require "backdoors" that weaken encryption, recognising that strong encryption helps protect human rights.
-

WHERE EACH CLAUSE COMES FROM

We keep a short map like this one in our notes. Then, in committee, we can answer any question about a clause with its source.

- Preambulatory clauses: Part 2 of the HMDC report (entries 33, 34, 35, 36 and 39 and the table in Section 2A), plus entries 2, 24, 27 and 40
 - Operative clauses 1 to 3: Solution 2 (entry 23); the European Parliament (entry 62) and entry 23; the White House (entry 63)
 - Operative clauses 4 to 6: Solution 4 (entry 28); the B-Tech Project (entry 37); Solution 4 (entry 27) and the funding problem (entry 45)
 - Operative clauses 7 to 9: entries 46 and 47; entries 51 and 52; Section 1C and entry 39
-

HOW WE MERGE AND AMEND IN COMMITTEE

1. **Merging with a binding-treaty bloc:** In 2014, China, Russia, India and many African states voted to begin writing a binding treaty on companies and human rights. France, Germany, Japan, the Republic of Korea, the United Kingdom and the United States voted against (United Nations Human Rights Council, July 14, 2014). If that bloc writes its own paper, we can offer a merge. We add a clause that welcomes the treaty talks, whose twelfth session was scheduled for October 12-16, 2026 (United Nations Human Rights Office, Last Accessed: October 2026). In return, they accept our clauses 1 and 4. That way, voluntary rules and future binding rules point the same way.
2. **Choosing words that can pass:** The African Union's Lusaka Declaration and India's domestic cloud pilot show that many states want "data sovereignty," meaning data kept under national control (Council on Foreign Relations, February 24, 2026). So we write clause 6 to let each country write its own law with UN help, instead of copying European rules. We also expect states that buy spyware for security work to accept clause 2 more easily than a full moratorium (a complete pause on sales).
3. **Amending through the right steps:** An amendment is a change to a draft resolution. If every sponsor agrees with it, it is a friendly amendment; if not, it is unfriendly and the committee must vote on it. We check the chair's exact rules for amendments on the first day. If one clause, such as clause 9 on encryption, threatens the whole paper, we can ask the committee to vote on that clause by itself. Then the rest of our resolution can still pass.

HMDC Forensics, Harvard MUN Online, December 2026
