

HMDC Presents... SPECPOL: Sample Position Paper

HMDC Presents... Sample Position Paper: SPECPOL: Corporate Surveillance, Accountability and Privacy

THIS IS A MODEL TO LEARN FROM, NOT TO COPY. We use this sample to see how one real country's facts fit into the four HMDC parts on a single page. We read it once for the ideas and a second time for the shape. Then we close it and write our own paper about our own country, in our own words. Even if one of us is assigned the Netherlands, we start again from our Country Report and never reuse these sentences.

THE SAMPLE PAPER

Committee: Special Political and Decolonization Committee (SPECPOL) **Topic:** Corporate Surveillance, Accountability and Privacy **Country:** The Kingdom of the Netherlands

Background of the Topic. The Kingdom of the Netherlands believes that corporate surveillance has become a global industry that no single country can control alone. At least 65 governments have acquired commercial spyware (software secretly placed on a phone to read messages and track its owner), and more than 500 companies reportedly sell surveillance tools to governments (United Nations Human Rights Office, August 4, 2022). This harm has reached Europe itself: researchers confirmed that spyware attacked the iPhones of two journalists in Italy in early 2025 without a single click (Citizen Lab, June 12, 2025). Meanwhile, data brokers buy, combine and sell personal records in deals that are mostly hidden and lightly limited by law (United Nations Human Rights Office, September 13, 2021). The root cause is the same in both cases: weak rules on who may sell surveillance and to whom.

UN and International Action. The Netherlands stands on Article 17 of the International Covenant on Civil and Political Rights (1966), which makes privacy a binding treaty right. It also stands on General Assembly resolution 68/167 (2013), the first resolution on the right to privacy in the digital age, adopted without a vote. Resolution 79/175 (2024) went further, expressing deep concern about the private surveillance industry and asking companies to collect data only with consent or a legal basis (United Nations General Assembly, December 17, 2024). Outside the UN, the Pall Mall Process wrote a voluntary Code of Practice for States, which 27 states had signed by December 2025 (National Cyber Security Centre, December 2, 2025). Yet these steps are voluntary for companies, and global internet freedom has now declined for the 15th year in a row (Freedom House, November 13, 2025).

Our Country's Policy. The national interests of the Netherlands are not open to compromise: human rights must be protected online just as they are offline, the founding idea of the Freedom Online Coalition, which began in The Hague in 2011 on Dutch initiative (Freedom Online Coalition, Last Accessed: October 2026), and Dutch data must stay safe from foreign control. For this reason, the Dutch Parliament passed eight motions in March 2025 to reduce reliance on United States technology firms (Council on Foreign Relations, February 24, 2026). Our policies, however, are open to negotiation. As a member of the European Union, the Netherlands applies EU export rules with human rights checks. Yet it does not ask other regions to copy European law word for word, and it accepts that states may use surveillance under strict legal conditions.

Proposed Solutions and Expected Opposition. First, the Netherlands proposes that every state add a human rights test of the receiving country to export licences for surveillance technology, as the UN Human Rights Office recommended (United Nations Human Rights Office, September 16, 2022). Second, it proposes a UN capacity-building programme for the roughly 57 countries that still lack data protection laws, since only 137 of 194 countries have them (UN Trade and Development, Last Accessed: October 2026). Third, it supports strict conditions on any state use of spyware: a judge's approval, a set purpose, a time limit and notice to targets afterward (European Parliament, June 15, 2023). The Netherlands expects states that buy spyware for security work to resist export tests, and it will answer that a human rights test leaves lawful trade open while closing the door to abuse.

HOW THIS SAMPLE IS BUILT

1. **Building the background from Part 1, Section 1A:** We chose three harms from the HMDC report's list: the size of the spyware market (entry 2), spyware on journalists' phones inside the EU (entry 8), and hidden data brokers (entry 11). We picked a European example on purpose. It shows that the problem is close to home for the Netherlands, not only far away.
2. **Choosing UN action from Part 2:** We did not list every resolution in the report's table (Section 2A). We picked the ICCPR (entry 34), resolution 68/167 (entry 35) and resolution 79/175 (entries 28 and 39). We added the Pall Mall Process from Part 3 (entry 53). Then we used Section 2C, "What Is Working and What Is Not," to point out the gap: nothing binds companies.
3. **Writing the policy from Part 3 and the bloc section:** The Freedom Online Coalition comes from entry 56, and the eight Dutch motions come from entry 64. The EU export rules come from entry 49 and the European Union paragraph in Section 2D. We kept the policy sentence general on purpose. The report does not say how the Netherlands voted in 2014 or which treaties it has ratified, and we never claim what our sources do not show.
4. **Separating interests from policies:** We wrote one firm sentence for the national interests and one flexible sentence for the policies we can negotiate. The flexible sentence tells other delegates exactly where the Netherlands can make a deal.
5. **Turning report solutions into proposals:** Each proposal comes from the report: export controls from Solution 2 (entry 23), data protection laws from Solution 4 (entry 27), and strict spyware conditions from the European Parliament entry in Part 3 (entry 62). The opposition sentence comes from the disadvantages listed under Solution 2.

HMDC Forensics, Harvard MUN Online, December 2026