

HMDC Presents... SPECPOL: Quick Guide

SPECPOL: QUICK GUIDE

Special Political and Decolonization Committee (SPECPOL): Corporate Surveillance, Accountability, and Privacy

WHAT WE ARE DEBATING

Corporate surveillance means companies watch people, or sell the tools that let governments watch them. Some companies sell spyware, which secretly takes over a phone. Others collect huge amounts of personal data through apps and cameras. We must decide who is responsible when a company's product hurts people.

WHAT OUR CHAIRS WILL FOCUS ON

Our chairs want us to show how private companies make surveillance possible. Then we build world rules that make those companies, and the governments that buy their tools, answer for harm. Our solutions must protect privacy and still keep countries safe, so each of us prepares one sentence on the security needs our country will defend.

FIVE NUMBERS TO REMEMBER

1. **189**: At least 189 journalists were targeted with Pegasus spyware. (United Nations Human Rights Office, August 4, 2022)
2. **74**: At least 74 governments bought spyware tools, and 30 were democracies. (Carnegie Endowment for International Peace, March 14, 2023)
3. **561**: Researchers mapped 561 companies and investors in the spyware market. (Atlantic Council, September 10, 2025)
4. **12 cents**: Data brokers sold private data about United States soldiers for 12 cents per record. (Sanford School of Public Policy, Duke University, November 2023)
5. **73 percent**: 73 percent of American adults said they have little or no control over their data. (Pew Research Center, October 18, 2023)

WHAT THE UN HAS ALREADY DONE

1. **A/HRC/RES/17/4 (2011)**: The Human Rights Council approved the Guiding Principles, which are rules companies may choose to follow.
2. **A/RES/68/167 (2013)**: The General Assembly passed its first digital privacy resolution, with no vote needed.
3. **A/HRC/RES/26/9 (2014)**: The Human Rights Council started work on a business treaty that companies must obey, in a split vote.

4. **A/RES/79/175 (2024):** The General Assembly named the private surveillance industry and listed what companies should do.
5. **A/RES/79/243 (2024):** The General Assembly adopted the Cybercrime Convention, which leaves each country's own laws to protect people.

THE MAIN SOLUTIONS

1. **A global moratorium on spyware sales:** All countries stop spyware sales for a while, until strong rules exist.
 - **Help:** It stops new abuses fastest.
 - **Harm:** Buyers may move to countries that ignore it.
2. **Stronger export controls:** A company needs a license, with a human rights check, to sell surveillance tools abroad.
 - **Help:** Many countries already have these systems.
 - **Harm:** Joining the main export group is a choice, and it was not built to protect human rights.
3. **A business and human rights treaty:** A treaty makes companies answer in law for human rights harms.
 - **Help:** It turns promises into law.
 - **Harm:** Talks have lasted over ten years without a final text.
4. **Data protection laws everywhere:** Every country adopts strong privacy laws for companies.
 - **Help:** It protects ordinary internet users.
 - **Harm:** Many poorer countries cannot pay to make companies obey them.

WHERE THE MAJOR BLOCS STAND

1. **The United States:** It banned risky spyware for its agencies, but its investors fund the spyware market most.
2. **The European Union:** It has the strongest rules, yet spyware abuse happened in Italy, Greece and Spain.
3. **China:** It voted in 2014 to start the business treaty.
4. **Russia:** It voted for the treaty, but pushes citizens to use a state-linked app that can take screenshots.
5. **The African Union and developing states:** Many voted for the treaty and want to depend less on big foreign technology companies.

KEY WORDS IN OUR TOPIC

1. **spyware:** When we say spyware, we mean hidden software that lets someone else read a phone's messages and track it.
2. **data broker:** When we say data broker, we mean a company that buys and sells information about people, usually secretly.
3. **zero-click attack:** When we say zero-click attack, we mean a hack that works even though the owner clicked nothing.

4. **export control:** When we say export control, we mean a rule that a company needs a license to sell certain products abroad.
5. **dual-use technology:** When we say dual-use technology, we mean a product that can protect or harm, depending on the user.
6. **moratorium:** When we say moratorium, we mean a temporary stop until rules are in place.
7. **encryption:** When we say encryption, we mean scrambling data so only the right person can read it.
8. **human rights due diligence:** When we say human rights due diligence, we mean a company checking carefully whether its products might cause harm.

QUESTIONS WE CAN ASK IN DEBATE

1. If a government spies on a journalist with a company's spyware, who is responsible: the company or the buyer?
2. Countries ignored earlier calls for a moratorium, so what would make a new call work?
3. Should every export license include a human rights test?
4. How can we help countries without privacy laws, without forcing European rules on them?

HMDC Forensics, Harvard MUN Online, December 2026

HMDC Forensics, Harvard MUN Online, December 2026