

HMDC Presents... SPECPOL: Part 3 (International Efforts)

HMDC Presents... Special Political and Decolonization Committee (SPECPOL): Corporate Surveillance, Accountability, and Privacy (Research Report, December 2026)

Prepared for Harvard Model United Nations Online, December 5-6, 2026. Every fact below sits inside an evidence entry that names its publication and date. All United Nations document symbols in this report were confirmed by opening the document on an official UN site (docs.un.org, documents.un.org, digitallibrary.un.org, un.org or ohchr.org).

WHAT OUR CHAIRS WILL FOCUS ON

Harvard tells us that this whole committee is about one hard trade: keeping countries safe while still protecting privacy and free speech, at a time when governments use AI and digital tools to watch for threats. The October session looks at how mass surveillance harms people's political freedom, but our December session moves to a different question: "the role of mass corporations in enabling surveillance." In December, we will be asked to show how private companies make surveillance possible and to build international standards that make those companies, and the governments that use their tools, accountable for privacy. Our final solutions must protect human rights and still respect real security needs.

Harvard Model United Nations, HMUN Online Committee Page, Last Accessed: October 2026
<https://www.harvardmun.org/specpol-online>

The parts of this report that match this focus most closely are the Introduction, the company and data-broker entries in Section 1A (entries 4, 5, 11, 12 and 19), Solutions 2, 3 and 4 in Section 1B, the business and human rights entries in Section 2B (entries 36, 37 and 39), and the international standards in Part 3 (entries 46 to 49, 52, 54 and 55).

How we use this report: Our report spends a lot of space on stories of spyware found on the phones of journalists and politicians (entries 7, 8, 9, 15 and 16), and those stories fit the October session's civil liberties focus more than December's. We use them as background examples only, and we always turn them back to the company that built and sold the tool. Harvard also asks us to balance privacy with national security, and our report covers the security side only briefly, mostly in the disadvantages lists under Solutions 2, 4 and 5 and in entry 48. So we prioritise company responsibility and international standards first, and we each prepare one sentence on what security needs our own country will defend.

PART 3, INTERNATIONAL EFFORTS

Beyond the UN, a patchwork of regional organizations, voluntary state groups, industry coalitions and university researchers works on this issue. The most binding rules come from Europe; the most global efforts are voluntary.

46. Council of Europe, Last Accessed: October 2026

Tagline: Building the first binding data treaty

Source: According to... Council of Europe, Last Accessed: October 2026

Link: <https://www.coe.int/en/web/data-protection/convention108-and-protocol>

Fact: It states... Convention 108, opened for signature on January 28, 1981, was the first legally binding international treaty on data protection, and parties must put its principles into their national law. An additional protocol from 2001 requires independent supervisory authorities, and a modernised version, Convention 108+, continues this work.

This means... a binding data protection treaty already exists and is open to countries outside Europe. Delegates can propose that more states join it rather than drafting a new UN treaty from nothing.

47. Council of Europe, May 21, 2026

Tagline: Nearing entry into force for Convention 108+

Source: According to... Council of Europe, May 21, 2026

Link: <https://www.coe.int/en/web/data-protection/-/republic-of-moldova-becomes-the-34th-state-to-ratify-the-convention-108->

Fact: It states... on May 15, 2026, the Republic of Moldova became the 34th state to ratify the protocol that modernises Convention 108 (known as Convention 108+). The modernised treaty needs 38 ratifications to enter into force, so four more are needed.

This means... the updated data protection treaty is close to becoming binding. A SPECPOL resolution could encourage states, including non-European ones, to ratify it and push it past the line.

48. Council of Europe, Last Accessed: October 2026

Tagline: Opening a global AI treaty

Source: According to... Council of Europe, Last Accessed: October 2026

Link: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>

Fact: It states... the Framework Convention on Artificial Intelligence opened for signature on September 5, 2024, and its signatories include the European Union, the United Kingdom, the United States, Canada, Israel, Japan and Uruguay. It covers private companies as well as governments and lists respect for privacy and data protection as a basic principle, but activities related to national security do not have to follow its provisions.

This means... this is the first international AI treaty, and it includes non-European countries. Its national security exemption, however, leaves out exactly the area where spyware is most used, which delegates should point out.

49. European Commission (Directorate-General for Trade), Last Accessed: October 2026

Tagline: Controlling surveillance exports in Europe

Source: According to... European Commission (Directorate-General for Trade), Last Accessed: October 2026

Link: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en

Fact: It states... the EU adopted Regulation (EU) 2021/821 on dual-use exports on May 20, 2021. It allows controls on items not on the official list when they could be used for human rights violations, lets member states add controls for human rights reasons, and the Commission consulted on cyber-surveillance guidance in 2023. The EU control list was updated again on September 14, 2026.

This means... the EU has written human rights into its export rules, which is a model for others. Carnegie's research (entry 3), however, found enforcement uneven across EU members.

50. Wassenaar Arrangement, June 17, 2025

Tagline: Coordinating dual-use export lists

Source: According to... Wassenaar Arrangement, June 17, 2025

Link: <https://www.wassenaar.org/about-us/>

Fact: It states... the Wassenaar Arrangement was agreed on December 19, 1995, has 42 participating states, and promotes transparency and responsibility in transfers of conventional arms and dual-use goods. Each participating state alone decides whether to allow or deny a transfer, and decisions are made by consensus.

This means... the main global export list depends on national choice and full agreement, so one state can block changes. Delegates proposing stronger export controls need to decide whether to work through Wassenaar or build something new.

51. Government of the United Kingdom (Pall Mall Process), February 6, 2024

Tagline: Launching the Pall Mall Process

Source: According to... Government of the United Kingdom, February 6, 2024

Link: <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>

Fact: It states... the United Kingdom and France hosted a conference in London that launched the Pall Mall Process, an ongoing global dialogue among governments, companies and civil society on the spread and irresponsible use of commercial cyber intrusion tools.

This means... the leading international effort on spyware sits outside the UN and is voluntary. SPECPOL can decide whether to welcome it, build on it, or bring it into the UN system.

52. Government of the United Kingdom (Pall Mall Process), April 4, 2025

Tagline: Writing a code for spyware buyers

Source: According to... Government of the United Kingdom, April 4, 2025

Link: <https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states>

Fact: It states... at the second Pall Mall meeting in Paris, April 3-4, 2025, a voluntary Code of Practice for States was launched, built on four pillars: accountability, precision, oversight and transparency. It covers states as regulators, customers and users of spyware. Named supporters include the United Kingdom, France, the United States, Romania, Finland, the Republic of Korea, Latvia and Belgium.

This means... a small group of mostly Western states has agreed on buyer rules, but it is non-binding and many major buyers are absent. Delegates can ask how to widen membership to the Global South.

53. National Cyber Security Centre (United Kingdom), December 2, 2025

Tagline: Asking the hacking industry for its own rules

Source: According to... National Cyber Security Centre (United Kingdom), December 2, 2025

Link: <https://www.ncsc.gov.uk/blog-post/what-makes-a-responsible-cyber-actor>

Fact: It states... the Pall Mall Process opened a consultation to write guidelines for the companies that find software flaws, build exploits and sell hacking services, in order to agree what responsible behaviour in this market looks like. By then, 27 states had signed the Code of Practice for States.

This means... the process is moving from rules for buyer governments to rules for sellers. Delegates can decide whether the UN should welcome these voluntary guidelines or call for binding ones.

54. Organisation for Economic Co-operation and Development (OECD), December 2022

Tagline: Limiting government access to company data

Source: According to... Organisation for Economic Co-operation and Development (OECD), December 2022

Link: <https://www.oecd.org/en/about/news/press-releases/2022/12/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.html>

Fact: It states... OECD countries adopted the first intergovernmental agreement on shared approaches to protecting privacy and other rights when governments access personal data held by companies for national security and law enforcement.

This means... the question of when governments may demand data from companies already has an agreed model among wealthy democracies. SPECPOL could encourage non-OECD states to adopt similar principles.

55. Global Network Initiative, Last Accessed: October 2026

Tagline: Joining companies and rights groups

Source: According to... Global Network Initiative, Last Accessed: October 2026

Link: <https://globalnetworkinitiative.org/about-gni/>

Fact: It states... the Global Network Initiative, launched in 2008, brings together technology companies, human rights and press freedom groups, academics and investors. It keeps principles and guidelines that help companies respond to government demands for censorship or user data, and it advocates for rights-respecting laws.

This means... some tech companies already accept outside rules on government data requests. Delegates can propose that more firms, including surveillance vendors, join similar initiatives.

56. Freedom Online Coalition, Last Accessed: October 2026

Tagline: Uniting governments for online rights

Source: According to... Freedom Online Coalition, Last Accessed: October 2026

Link: <https://freedomonlinecoalition.com/about-us/about/>

Fact: It states... the Freedom Online Coalition was founded in 2011 in The Hague on the initiative of the Netherlands and has grown from 15 to 41 member states. Its members hold that human rights people have offline must also be protected online.

This means... there is a ready-made group of governments that could sponsor or co-sponsor a SPECPOL resolution. Delegates from member states can use it to build a bloc.

57. TechCrunch, October 18, 2025

Tagline: Holding a spyware company liable in court

Source: According to... TechCrunch, October 18, 2025

Link: <https://techcrunch.com/2025/10/18/spyware-maker-nso-group-blocked-from-whatsapp>

Fact: It states... on October 17, 2025, United States District Judge Phyllis Hamilton issued a permanent injunction (a court order) barring NSO Group from targeting WhatsApp users. The case concerned a 2019 campaign against more than 1,400 WhatsApp users, including journalists and human rights activists. A jury had earlier in 2025 ordered NSO to pay more than 167 million US dollars, but the judge reduced the payment to about 4 million.

This means... a private company used a national court to hold a spyware maker responsible, something no UN body has done. Delegates can debate whether individual victims in other countries should have a similar path to court.

58. Citizen Lab (University of Toronto), September 18, 2018

Tagline: Detecting spyware across 45 countries

Source: According to... Citizen Lab (University of Toronto), September 18, 2018

Link: <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

Fact: It states... researchers found suspected Pegasus operations in 45 countries, grouped into 36 separate operators, at least 10 of which appeared to spy across borders. Six countries with major Pegasus activity had earlier been linked to spyware abuse against civil society.

This means... much of what the world knows about spyware comes from independent university researchers, not governments. Delegates may propose protecting and funding this kind of independent technical research.

59. Freedom House, Last Accessed: October 2026

Tagline: Measuring the decline of internet freedom

Source: According to... Freedom House, Last Accessed: October 2026

Link: <https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online>

Fact: It states... in its Freedom on the Net 2024 report, covering June 2023 to May 2024, Freedom House found global internet freedom declined for the 14th year in a row. Of the 72 countries studied, which hold 87 percent of the world's internet users, 27 declined and 18 improved.

This means... the overall trend is moving away from online freedom, not toward it. Delegates can use this to argue that current international efforts are not enough.

60. Freedom House, November 13, 2025

Tagline: Recording a fifteenth year of decline

Source: According to... Freedom House, November 13, 2025

Link: <https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet>

Fact: It states... Freedom on the Net 2025, covering June 2024 to May 2025, found that global internet freedom declined for the 15th year in a row. Of 72 countries holding 89 percent of the world's internet users, 28 declined and 17 improved. Between January 2020 and March 2025, 17 of the 72 countries blocked encrypted messaging apps, and Serbian authorities used Cellebrite phone-extraction tools to search the phones of journalists and activists.

This means... the decline described in the 2024 report continued. Tools sold by private companies, such as phone-extraction software, keep appearing in cases against journalists, which supports stronger controls on who may buy them.

61. Carnegie Endowment for International Peace, September 17, 2019

Tagline: Indexing AI surveillance worldwide

Source: According to... Carnegie Endowment for International Peace, September 17, 2019

Link: <https://carnegieendowment.org/features/ai-global-surveillance-technology>

Fact: It states... Carnegie's AI Global Surveillance Index studied 176 countries and lists 75 countries using AI surveillance technology. Its data comes from 2018-2019 sources.

This means... AI surveillance was already widespread years ago, and the figure is likely higher today. Delegates should treat 75 countries as a minimum, not a current total.

62. European Parliament, June 15, 2023

Tagline: Setting European conditions for spyware use

Source: According to... European Parliament, June 15, 2023

Link: <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse>

Fact: It states... the European Parliament adopted the recommendations of its spyware inquiry (the PEGA committee) by 411 votes to 97, with 37 abstentions. It asked Hungary and Poland to restore judicial independence and require independent judicial approval before spyware is used, asked Greece and Cyprus to cancel export licences that break EU rules, and asked Spain to investigate 47 cases in which it is unknown who authorised the spying. It said police use of spyware should be limited to exceptional cases, a set purpose and a short time, that targets should be notified afterwards, and it proposed an independent EU Tech Lab to investigate surveillance and screen devices.

This means... Europe chose strict conditions rather than a full ban. Delegates can borrow this list (a judge's approval, time limits, notifying targets, an independent lab) as ready-made language for a resolution.

63. The White House, March 27, 2023

Tagline: Barring risky spyware from a government's own agencies

Source: According to... The White House, March 27, 2023

Link: <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/>

Fact: It states... the United States President ordered that federal agencies shall not make operational use of commercial spyware that poses significant counterintelligence or security risks, or significant risks of improper use by a foreign government. The order says foreign governments have used commercial spyware to target perceived opponents, curb dissent, limit freedom of expression and track people without proper legal authorization. This page is kept in the official archive of the previous administration.

This means... a major buyer can shrink the market by refusing to buy from abusive vendors. Delegates can propose that other states adopt similar purchasing rules, while noting that a presidential order can be changed by a later president.

64. Council on Foreign Relations, February 24, 2026

Tagline: Seeking digital independence from foreign companies

Source: According to... Council on Foreign Relations, February 24, 2026

Link: <https://www.cfr.org/articles/americas-digital-empire-has-a-trust-problem>

Fact: It states... three United States companies, Amazon Web Services, Microsoft Azure and Google Cloud, control nearly two-thirds of global cloud services, and four large firms hold more than 70 percent of international undersea cable capacity. Fearing that Washington could force these firms to follow its orders, other countries are trying to depend on them less: India's central bank approved a domestic cloud pilot in late 2024, the Dutch Parliament passed eight motions to cut reliance on United States tech firms in March 2025, and in July 2025 the African Union's legislative body adopted the Lusaka Declaration.

This means... many states now see dependence on a few foreign companies as a privacy and security risk in itself. Delegates from the Global South can argue for "data sovereignty" (keeping data under national control), while others may warn that smaller national systems can be less secure.

KEY VOCABULARY

1. **Spyware:** Software secretly installed on a phone or computer that lets someone else read messages, track location and switch on the camera or microphone.
 2. **Commercial spyware / surveillance-for-hire:** Spyware built by private companies and sold to governments or others for profit.
 3. **Zero-click attack:** A hack that infects a device without the owner clicking anything.
 4. **Zero-day exploit:** An attack that uses a software flaw the maker does not yet know about, so no fix exists.
 5. **Data broker:** A company that buys, combines and sells personal information about people, usually without their knowledge.
 6. **Biometric data:** Information about a person's body, such as face, fingerprints or voice, used to identify them.
 7. **Export control:** A government rule requiring a license before certain products can be sold to other countries.
 8. **Dual-use technology:** A product that can be used for both peaceful and harmful purposes, such as software that protects networks or attacks them.
 9. **Moratorium:** A temporary stop on an activity until certain conditions are met.
 10. **Human rights due diligence:** The process a company uses to find, prevent and address human rights harms its products or operations may cause.
 11. **Encryption:** Scrambling data so only the intended person can read it.
 12. **UN Guiding Principles on Business and Human Rights (UNGPs):** The 2011 UN framework stating that states must protect, companies must respect, and victims must have access to remedy.
-

DISCUSSION QUESTIONS

1. When a company sells spyware to a government that then uses it against a journalist in another country, who should be held responsible: the company, the company's home country, the buying government, or all three?
2. Should the UN call for a global moratorium on commercial spyware, even though the 2019 and 2021 calls were largely ignored? What would make a new call more effective?
3. Should export controls on surveillance technology include a mandatory human rights test? Should that be done through the Wassenaar Arrangement or a new body?
4. Is it time to make the UN Guiding Principles binding on technology companies, or would a binding treaty push companies to move to countries that refuse to join?
5. How can developing countries, about 57 of which lack data protection laws, be helped to protect their citizens without being forced to copy European rules?
6. Should states be allowed to use spyware at all? If yes, under what conditions (for example, a judge's approval, a serious crime, a time limit)?
7. How should the UN Convention against Cybercrime be applied so that cross-border evidence sharing does not help governments spy on critics?

8. Should the UN create a way for surveillance victims to get compensation from foreign companies, and how would it be funded during the UN's cash crisis?
-

Research Notes and Gaps

- The web search budget was used up early in this research session, so all sources were reached by opening known official addresses directly. This limited the number of major news sources (Reuters, AP, BBC); several news and NGO pages refused automated access and are not cited.
- The 2025 jury verdict and court order against NSO Group in the WhatsApp case are now cited (entry 57). The 2023 European fine against Meta could not be opened and is not cited.
- No Human Rights Council privacy resolution was found at the 60th session (2025), and no General Assembly privacy resolution is expected before the 81st session, since it is adopted every two years.
- The Hanoi signing count (72 countries, entry 43) and the Convention 108+ ratification count (34 of the 38 needed as of May 2026, entry 47) are now cited. Current totals change often; delegates should check the UN Treaty Collection and the Council of Europe Treaty Office before the conference.
- The Carnegie AI Global Surveillance Index data dates from 2018-2019 and should be treated as historical.
- Third research round (October 14, 2026): twelve entries were added (15-20, 31, 32, 44, 62-64), mostly from 2026, along with the bloc section (Section 2D). Exact publication dates replaced "Last Accessed" for entries 30, 50 and 61. The remaining "Last Accessed" pages (UN, Council of Europe, UNCTAD, OHCHR and coalition reference pages) show no publication date of their own.
- Remaining gaps: no Reuters, BBC, Chatham House, RAND or IISS page could be opened (they refused automated access), and a detailed Chinese government statement on commercial spyware was not found. The 76-signer Cybercrime Convention count (entry 44) dates from May 2026; check the UN Treaty Collection for the current number of signers and parties. The 2023 United States executive order (entry 63) comes from the previous administration's archive, and delegates should check whether it is still in effect.