

HMDC Presents... SPECPOL: Part 2 (The United Nations)

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 2, THE UNITED NATIONS RECORD

The United Nations has worked on digital privacy since 2013, mainly through the General Assembly's Third Committee and the Human Rights Council in Geneva. Its record is strong on setting standards and weak on enforcement: it has produced many resolutions and reports, but none of them creates binding duties for companies.

Section 2A: Table of UN Resolutions and Instruments

Every symbol below was confirmed by opening the document on an official UN site.

Symbol	Year	Body	What it does (one plain sentence)
A/RES/217 A (III)	1948	General Assembly	Adopts the Universal Declaration of Human Rights, whose Article 12 protects against arbitrary interference with privacy.
A/RES/2200 A (XXI)	1966	General Assembly	Adopts the International Covenant on Civil and Political Rights, whose Article 17 makes privacy a binding treaty right.
A/HRC/RES/17/4	2011	Human Rights Council	Endorses the UN Guiding Principles on Business and Human Rights ("Protect, Respect and Remedy").
A/RES/68/167	2013	General Assembly	First resolution on the right to privacy in the digital age, adopted without a vote.
A/HRC/RES/26/9	2014	Human Rights Council	Creates a working group to draft a legally binding treaty on transnational corporations and human rights (vote 20-14-13).
A/RES/69/166	2014	General Assembly	Second resolution on the right to privacy in the digital age.
A/HRC/RES/28/16	2015	Human Rights Council	Creates the Special Rapporteur on the right to privacy for three years.
A/RES/71/199	2016	General Assembly	Updates the right to privacy in the digital age resolution.
A/HRC/RES/34/7	2017	Human Rights Council	Asks the High Commissioner to hold an expert workshop on privacy principles and best practices.
A/HRC/RES/37/2	2018	Human Rights Council	Extends the Special Rapporteur on privacy mandate for three more

			years.
A/RES/73/179	2018	General Assembly	Updates the right to privacy in the digital age resolution.
A/HRC/RES/41/11	2019	Human Rights Council	Opens work on new and emerging digital technologies and human rights, including a panel discussion.
A/HRC/RES/42/15	2019	Human Rights Council	Asks for an expert seminar on how AI and profiling affect privacy, leading to report A/HRC/48/31.
A/RES/75/176	2020	General Assembly	Updates the right to privacy in the digital age resolution.
A/HRC/RES/46/16	2021	Human Rights Council	Renews the mandate of the Special Rapporteur on the right to privacy.
A/HRC/RES/48/4	2021	Human Rights Council	Asks the UN Human Rights Office for a report on new privacy trends, leading to A/HRC/51/17 on spyware.
A/RES/77/211	2022	General Assembly	Updates the right to privacy in the digital age resolution.
A/HRC/RES/53/29	2023	Human Rights Council	Asks the UN Human Rights Office to keep applying the Guiding Principles to technology companies.
A/HRC/RES/54/21	2023	Human Rights Council	Expresses concern about spyware from the private surveillance industry and asks for a report on data and discrimination (A/HRC/60/45).
A/RES/78/213	2023	General Assembly	Addresses human rights in the context of digital technologies, including unlawful surveillance and the private surveillance industry.
A/RES/78/265	2024	General Assembly	First General Assembly resolution on safe, secure and trustworthy AI, noting privacy risks.
A/HRC/RES/55/3	2024	Human Rights Council	Renews the Special Rapporteur on privacy mandate again.
A/RES/78/311	2024	General Assembly	Promotes international cooperation on capacity-

			building in artificial intelligence.
A/RES/79/1	2024	General Assembly	Adopts the Pact for the Future and the Global Digital Compact, including commitments on data protection and lawful surveillance.
A/RES/79/175	2024	General Assembly	Latest right to privacy in the digital age resolution, with detailed calls on businesses and concern about the private surveillance industry.
A/RES/79/243	2024	General Assembly	Adopts the UN Convention against Cybercrime, with human rights safeguards in Articles 6 and 24.
A/HRC/RES/58/23	2025	Human Rights Council	Addresses risks that digital technologies, including surveillance and tracking, create for human rights defenders.
A/HRC/RES/59/11	2025	Human Rights Council	Asks the UN Human Rights Office to expand system-wide work on human rights in new digital technologies.
A/RES/79/325	2025	General Assembly	Sets up the Independent International Scientific Panel on AI and the Global Dialogue on AI Governance.

Section 2B: Evidence on What the UN Has Done

33. United Nations (UDHR page), Last Accessed: October 2026

Tagline: Grounding privacy in the Universal Declaration

Source: According to... United Nations, Last Accessed: October 2026

Link: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

Fact: It states... the Universal Declaration of Human Rights, adopted on December 10, 1948, by General Assembly resolution 217 A (III), says in Article 12 that no one shall face arbitrary interference with their privacy, family, home or correspondence, and that everyone has the right to legal protection against it.

This means... privacy is one of the oldest rights in the UN system. Delegates can argue that digital surveillance is a new form of an old violation, not a new issue that needs new permission to regulate.

34. United Nations Human Rights Office (ICCPR page), Last Accessed: October 2026

Tagline: Making privacy a treaty right

Source: According to... United Nations Human Rights Office, Last Accessed: October 2026

Link: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

Fact: It states... the International Covenant on Civil and Political Rights, adopted by resolution 2200 A (XXI) on December 16, 1966, and in force since March 23, 1976, says in Article 17 that no one may face arbitrary or unlawful interference with privacy or correspondence, and that everyone is entitled to legal protection against it.

This means... states that joined this treaty have a legal duty to protect privacy, including against private actors. Delegates can use this to argue that states must regulate companies, not just restrain their own spies.

35. United Nations Digital Library (A/RES/68/167), January 21, 2014

Tagline: Starting the digital privacy agenda

Source: According to... United Nations Digital Library, January 21, 2014

Link: <https://digitallibrary.un.org/record/764407>

Fact: It states... the General Assembly adopted resolution 68/167, "The right to privacy in the digital age," without a vote on December 18, 2013, during its 68th session.

This means... the UN's modern digital privacy work began with full consensus. Every two years since, the Assembly has updated this resolution, which gives SPECPOL a long line of agreed language to build on.

36. United Nations Human Rights Council (A/HRC/RES/17/4), July 6, 2011

Tagline: Endorsing the Guiding Principles

Source: According to... United Nations Human Rights Council (Resolution A/HRC/RES/17/4), July 6, 2011

Link: <https://docs.un.org/en/A/HRC/RES/17/4>

Fact: It states... the Council endorsed the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. These principles say states must protect people from business abuses, companies must respect human rights, and victims must have access to remedy.

This means... the UN's main tool for corporate accountability is voluntary for companies. Almost every later privacy resolution points back to these principles, so delegates should understand them before proposing anything stronger.

37. United Nations Human Rights Office (B-Tech Project), Last Accessed: October 2026

Tagline: Applying the Guiding Principles to tech

Source: According to... United Nations Human Rights Office, Last Accessed: October 2026

Link: <https://www.ohchr.org/en/business-and-human-rights/b-tech-project>

Fact: It states... the UN Human Rights Office launched the B-Tech Project in 2019 to give technology companies, states and investors authoritative guidance on applying the Guiding Principles in the tech sector, and it has worked with all of them since then.

This means... the UN already has a dedicated program that speaks directly to tech firms. Delegates can propose to expand B-Tech's role, for example by asking it to write specific guidance for surveillance technology sellers.

38. United Nations Human Rights Office (Special Rapporteur on Privacy), Last Accessed: October 2026

Tagline: Creating a privacy watchdog

Source: According to... United Nations Human Rights Office, Last Accessed: October 2026

Link: <https://www.ohchr.org/en/special-procedures/sr-privacy>

Fact: It states... the Human Rights Council created the Special Rapporteur on the right to privacy in 2015 through resolution 28/16, and renewed it for three years in March 2024. The current mandate holder is Dr. Ana Brian Nougrères of Uruguay, in office since August 1, 2021. The role includes reviewing surveillance laws and setting out the private sector's responsibilities.

This means... there is one UN expert focused on privacy, but she can investigate and recommend, not enforce. Delegates may debate whether this office needs more resources or more power.

39. United Nations General Assembly (A/RES/79/175), December 17, 2024

Tagline: Naming the private surveillance industry

Source: According to... United Nations General Assembly (Resolution A/RES/79/175), December 17, 2024

Link: <https://docs.un.org/en/A/RES/79/175>

Fact: It states... the General Assembly expressed deep concern about tools developed by the private surveillance industry to hack devices, intercept communications and collect data on human rights defenders and journalists. It also stressed that companies should respect privacy when collecting biometric information, and that strong encryption and anonymity help protect human rights.

This means... the Assembly has formally named the industry at the centre of this topic. SPECPOL can treat this as agreed language and move to the harder question of what to do about it.

40. United Nations General Assembly (A/RES/79/1), September 22, 2024

Tagline: Committing to data protection in the Global Digital Compact

Source: According to... United Nations General Assembly (Resolution A/RES/79/1), September 22, 2024

Link: <https://docs.un.org/en/A/RES/79/1>

Fact: It states... in the Global Digital Compact, annexed to the Pact for the Future, world leaders recognized that growing data collection, including in AI systems, may increase risks without effective data protection and privacy rules. They 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.

This means... heads of state have already promised capacity-building and lawful surveillance at the highest level. Delegates can ask how these promises will be measured, which is a gap in the Compact.

41. United Nations General Assembly (A/RES/79/243), December 24, 2024

Tagline: Adding safeguards to the Cybercrime Convention

Source: According to... United Nations General Assembly (Resolution A/RES/79/243), December 24, 2024

Link: <https://docs.un.org/en/A/RES/79/243>

Fact: It states... the UN Convention against Cybercrime requires that states implement it consistently with international human rights law (Article 6), and that its investigative powers be subject to conditions and safeguards in domestic law that protect human rights (Article 24). Nothing in it may be read as permitting the suppression of freedom of expression or peaceful assembly.

This means... the newest UN treaty that touches surveillance relies on each country's own laws for protection. Where domestic laws are weak, those safeguards are weak too, so delegates should debate whether the treaty's evidence-sharing powers need extra international limits.

42. UN Office on Drugs and Crime, Last Accessed: October 2026

Tagline: Opening the Cybercrime Convention for signature

Source: According to... United Nations Office on Drugs and Crime (UNODC), Last Accessed: October 2026

Link: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>

Fact: It states... the Convention was opened for signature on October 25, 2025, at a ceremony in Hanoi, Viet Nam, and will enter into force after 40 states become parties.

This means... the treaty is not yet in force, so how it will be applied is still open. SPECPOL could recommend how states should protect privacy when they share data under it.

43. Just Security (New York University School of Law), November 20, 2025

Tagline: Counting the first Cybercrime Convention signers

Source: According to... Just Security (New York University School of Law), November 20, 2025

Link: <https://www.justsecurity.org/124057/promise-peril-cybercrime-convention/>

Fact: It states... 72 countries signed the UN Convention against Cybercrime at the Hanoi ceremony in late October 2025, including the European Union as a bloc, 13 EU member states, the United Kingdom and Australia. The United States, Canada, Japan, India, Israel and New Zealand did not sign there. Critics warn that the treaty gives broad surveillance powers that reach beyond computer crime while its human rights safeguards are weak, and a dozen human rights groups urged states not to sign.

This means... the treaty has wide but incomplete support, and several major technology countries are staying out for now. Delegates can debate what extra privacy protections would bring the remaining states in.

44. UN News, May 4, 2026

Tagline: Adding signers and a permanent cyber forum

Source: According to... UN News, May 4, 2026

Link: <https://news.un.org/en/story/2026/05/1167439>

Fact: It states... by May 2026, 76 UN Member States had signed the UN Convention against Cybercrime. The article, written by the Director of the UN Institute for Disarmament Research, also explains that the General Assembly endorsed 11 voluntary norms of responsible state behaviour in cyberspace in 2015 and reaffirmed them in 2021, and that a new UN Global Mechanism on Information and Communications Technology would launch in the coming months as a single permanent track for governments.

This means... support for the cybercrime treaty grew from 72 signers in Hanoi (entry 43) to 76, but signing is not the same as joining: the treaty enters into force only after 40 states become parties. The new permanent mechanism also gives SPECPOL a UN forum it can ask to take up surveillance questions.

45. United Nations Human Rights Office (A/HRC/60/45), August 29, 2025

Tagline: Revealing a funding problem

Source: According to... United Nations Human Rights Office (Report A/HRC/60/45), August 29, 2025

Link: <https://docs.un.org/en/A/HRC/60/45>

Fact: It states... this privacy report, requested by the Human Rights Council for its 57th session, had to be postponed to the 60th session because of the liquidity (cash) crisis affecting the UN Secretariat.

This means... the UN's privacy work is slowed by a lack of money, not only a lack of political will. Any resolution that asks the UN for new reports or offices must explain how they will be funded.

Section 2C: What Is Working and What Is Not

Working (helping): - Clear, agreed standards: the right to privacy in the digital age resolution has been updated every two years since 2013, and its language on businesses has grown more detailed (entries 28, 35, 39). - Expert investigation: OHCHR reports have documented spyware harms in detail and given states concrete recommendations (entries 1, 2, 10, 23). - A permanent privacy expert: the Special Rapporteur mandate has been renewed three times (entry 38).

Not working (undesirable results): - No binding duties on companies: the Guiding Principles and the Assembly's calls on business remain voluntary (entries 28, 36). - Moratorium calls ignored: UN experts asked for a pause in 2019 and again in 2021, with little action (entry 21). - Slow treaty talks: the binding business and human rights treaty has been under negotiation since 2014 (entries 25, 26). - Money shortages: reports are delayed by the UN liquidity crisis (entry 45).

Section 2D: WHERE THE MAJOR BLOCS STAND

States do not split neatly into "for privacy" and "against privacy." Many governments that criticize spyware abroad also buy surveillance tools at home, so delegates should expect every bloc to defend some forms of surveillance while attacking others. The positions below come from public votes, laws and reporting; delegates should check their own country's latest statement before the conference.

1. **The United States:** In 2023 the United States barred its own federal agencies from using commercial spyware that poses security risks or that foreign governments have misused, and it backs the Pall Mall Code of Practice (entry 52). At the same time, United States investors are now the largest funders in the spyware market (entry 5), and the United States voted against starting a binding business and human rights treaty in 2014 (entry 25).
 - Source: According to... The White House, March 27, 2023 (entry 63)
 - 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/>
2. **The European Union:** The EU has the strongest regional rules, including AI Act bans (entry 30), human rights checks on exports (entry 49) and the European Parliament's strict conditions for spyware use (entry 62). Yet spyware abuse has been documented inside EU members such as Italy, Greece, Hungary, Poland and Spain, and several EU states voted against the binding business treaty in 2014.
 - Source: According to... European Parliament, June 15, 2023 (entry 62)
 - Link: <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse>
3. **China:** China voted in favour of creating the working group to write a binding treaty on transnational corporations and human rights in 2014, alongside Russia, India and many African states. A detailed Chinese statement on commercial spyware was not found in a source opened for this report, so delegates representing China should check its recent Third Committee speeches.
 - Source: According to... United Nations Human Rights Council (Resolution A/HRC/RES/26/9), July 14, 2014 (entry 25)
 - Link: <https://docs.un.org/en/A/HRC/RES/26/9>
4. **Russia:** Russia also voted for the binding business treaty in 2014. At home, tens of millions of Russians have been pushed to install Max, a state-linked "super-app" that researchers at the University of Michigan found can take screenshots of a user's device and reach the messages and payments inside its mini-apps, while Russia has banned WhatsApp and Telegram.
 - Source: According to... The Guardian, September 18, 2026
 - Link: <https://www.theguardian.com/world/2026/sep/18/russian-super-app-max-spy-citizens>
5. **The African Union and the developing world (G77 and China):** In the 2014 vote, Algeria, Kenya, South Africa, Ethiopia, Indonesia, Pakistan, the Philippines and Viet Nam all voted for the binding treaty, while Brazil, Mexico and Argentina abstained. In July 2025, the African Union's legislative body adopted the Lusaka Declaration, calling for "a secure, inclusive, sovereign digital and AI future" that depends less on foreign technology giants.
 - Source: According to... Council on Foreign Relations, February 24, 2026 (entry 64)
 - Link: <https://www.cfr.org/articles/americas-digital-empire-has-a-trust-problem>

6. **India:** India voted for the binding business treaty in 2014 and did not sign the UN Convention against Cybercrime at the Hanoi ceremony in 2025 (entry 43). Its central bank has also tested a domestic cloud service to reduce reliance on Silicon Valley (entry 64), which shows a strong interest in keeping data under national control.
- Source: According to... Just Security (New York University School of Law), November 20, 2025 (entry 43)
 - Link: <https://www.justsecurity.org/124057/promise-peril-cybercrime-convention/>
-