

HMDC Presents... SPECPOL: Full Report

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.

TABLE OF CONTENTS

- **Introduction: What This Committee Is Deciding**

- **PART 1, THE TOPIC: HARMS AND SOLUTIONS**

- Section 1A: The Harms

- 1. United Nations Human Rights Office (A/HRC/51/17), August 4, 2022: Counting the victims of Pegasus
 - 2. United Nations Human Rights Office (A/HRC/51/17), August 4, 2022: Measuring the size of the spyware market
 - 3. Carnegie Endowment for International Peace, March 14, 2023: Mapping which governments buy spyware
 - 4. Atlantic Council, September 4, 2024: Tracing the companies behind spyware
 - 5. Atlantic Council, September 10, 2025: Following new money into spyware
 - 6. Google Threat Analysis Group, February 6, 2024: Linking vendors to zero-day attacks
 - 7. Citizen Lab (University of Toronto), March 19, 2025: Exposing a newer spyware vendor
 - 8. Citizen Lab (University of Toronto), June 12, 2025: Confirming spyware on journalists' phones
 - 9. UN Special Rapporteur on Freedom of Expression (A/HRC/41/35), May 28, 2019: Connecting surveillance to detention and torture
 - 10. United Nations Human Rights Office (A/HRC/51/17), August 4, 2022: Watching public spaces through cameras
 - 11. United Nations Human Rights Office (A/HRC/48/31), September 13, 2021: Explaining how data brokers operate
 - 12. Sanford School of Public Policy, Duke University, November 2023: Buying soldiers' personal data cheaply
 - 13. United Nations Human Rights Office (A/HRC/60/45), August 29, 2025: Showing who is harmed most
 - 14. Pew Research Center, October 18, 2023: Measuring public distrust of companies
 - 15. The Guardian, September 3, 2026: Recording Serbia's largest wave of spyware attacks
 - 16. Citizen Lab (University of Toronto), July 3, 2026: Hacking a lawmaker who investigated spyware
 - 17. PBS NewsHour (Associated Press), March 23, 2026: Turning street cameras into a weapon
 - 18. Center for Strategic and International Studies (CSIS), September 16, 2026: Combining stolen data with AI
 - 19. Brookings Institution, May 20, 2026: Showing how governments buy company tools
 - 20. The Guardian, August 3, 2026: Pressing a company to weaken encryption

- Section 1B: Major Potential Solutions
 - Solution 1: A Global Moratorium on Spyware Sales
 - 21. UN Human Rights Experts (OHCHR), August 12, 2021: Demanding a global moratorium
 - 22. Carnegie Endowment for International Peace, March 14, 2023: Warning that buyers switch suppliers
 - Solution 2: Stronger Export Controls on Surveillance Technology
 - 23. United Nations Human Rights Office (OHCHR press release), September 16, 2022: Calling for export control regimes
 - 24. UN Special Rapporteur on Freedom of Expression (A/HRC/41/35), May 28, 2019: Showing the limits of Wassenaar
 - Solution 3: A Binding Treaty on Business and Human Rights
 - 25. United Nations Human Rights Council (A/HRC/RES/26/9), July 14, 2014: Launching the binding treaty process
 - 26. United Nations Human Rights Office (OEIGWG page), Last Accessed: October 2026: Tracking slow treaty negotiations
 - Solution 4: Comprehensive Data Protection Laws Everywhere
 - 27. UN Trade and Development (UNCTAD), Last Accessed: October 2026: Counting countries with privacy laws
 - 28. United Nations General Assembly (A/RES/79/175), December 17, 2024: Listing what companies must do
 - Solution 5: Banning the Most Dangerous AI Surveillance Uses
 - 29. United Nations Human Rights Office (A/HRC/48/31), September 13, 2021: Recommending bans and moratoriums
 - 30. European Commission, August 3, 2026: Showing a regional ban in action
 - 31. The Guardian, September 29, 2026: Testing facial recognition in train stations
 - 32. The Guardian, October 5, 2026: Pausing smart glasses in public places
 - Section 1C: Lesser Solutions (brief list)

- **PART 2, THE UNITED NATIONS RECORD**

- Section 2A: Table of UN Resolutions and Instruments
- Section 2B: Evidence on What the UN Has Done
 - 33. United Nations (UDHR page), Last Accessed: October 2026: Grounding privacy in the Universal Declaration
 - 34. United Nations Human Rights Office (ICCPR page), Last Accessed: October 2026: Making privacy a treaty right
 - 35. United Nations Digital Library (A/RES/68/167), January 21, 2014: Starting the digital privacy agenda
 - 36. United Nations Human Rights Council (A/HRC/RES/17/4), July 6, 2011: Endorsing the Guiding Principles
 - 37. United Nations Human Rights Office (B-Tech Project), Last Accessed: October 2026: Applying the Guiding Principles to tech
 - 38. United Nations Human Rights Office (Special Rapporteur on Privacy), Last Accessed: October 2026: Creating a privacy watchdog
 - 39. United Nations General Assembly (A/RES/79/175), December 17, 2024: Naming the private surveillance industry
 - 40. United Nations General Assembly (A/RES/79/1), September 22, 2024: Committing to data protection in the Global Digital Compact
 - 41. United Nations General Assembly (A/RES/79/243), December 24, 2024: Adding safeguards to the Cybercrime Convention
 - 42. UN Office on Drugs and Crime, Last Accessed: October 2026: Opening the Cybercrime Convention for signature
 - 43. Just Security (New York University School of Law), November 20, 2025: Counting the first Cybercrime Convention signers
 - 44. UN News, May 4, 2026: Adding signers and a permanent cyber forum
 - 45. United Nations Human Rights Office (A/HRC/60/45), August 29, 2025: Revealing a funding problem
- Section 2C: What Is Working and What Is Not
- Section 2D: Where the Major Blocs Stand (the United States, the European Union, China, Russia, the African Union and developing states, India)

• PART 3, INTERNATIONAL EFFORTS

- 46. Council of Europe, Last Accessed: October 2026: Building the first binding data treaty
- 47. Council of Europe, May 21, 2026: Nearing entry into force for Convention 108+
- 48. Council of Europe, Last Accessed: October 2026: Opening a global AI treaty
- 49. European Commission (Directorate-General for Trade), Last Accessed: October 2026: Controlling surveillance exports in Europe
- 50. Wassenaar Arrangement, June 17, 2025: Coordinating dual-use export lists
- 51. Government of the United Kingdom (Pall Mall Process), February 6, 2024: Launching the Pall Mall Process
- 52. Government of the United Kingdom (Pall Mall Process), April 4, 2025: Writing a code for spyware buyers
- 53. National Cyber Security Centre (United Kingdom), December 2, 2025: Asking the hacking industry for its own rules
- 54. Organisation for Economic Co-operation and Development (OECD), December 2022: Limiting government access to company data
- 55. Global Network Initiative, Last Accessed: October 2026: Joining companies and rights groups
- 56. Freedom Online Coalition, Last Accessed: October 2026: Uniting governments for online rights
- 57. TechCrunch, October 18, 2025: Holding a spyware company liable in court
- 58. Citizen Lab (University of Toronto), September 18, 2018: Detecting spyware across 45 countries
- 59. Freedom House, Last Accessed: October 2026: Measuring the decline of internet freedom
- 60. Freedom House, November 13, 2025: Recording a fifteenth year of decline
- 61. Carnegie Endowment for International Peace, September 17, 2019: Indexing AI surveillance worldwide
- 62. European Parliament, June 15, 2023: Setting European conditions for spyware use
- 63. The White House, March 27, 2023: Barring risky spyware from a government's own agencies
- 64. Council on Foreign Relations, February 24, 2026: Seeking digital independence from foreign companies

• KEY VOCABULARY

• DISCUSSION QUESTIONS

• Research Notes and Gaps

Introduction: What This Committee Is Deciding

Corporate surveillance is the collection, tracking and analysis of people's lives by private companies, or by governments using tools that private companies build and sell. It has two faces. The first is the **spyware industry**: firms that sell hacking tools to governments, which sometimes use them against journalists, opposition politicians and human rights defenders. The second is the **data economy**: apps, platforms, camera networks and data brokers that collect huge amounts of personal information, which can then be sold, leaked or handed to governments.

SPECPOL handles political questions that cross borders. In this committee, delegates will argue about three linked questions. Who should be held responsible when a company's product is used to harm people in another country? What international rules, if any, should control the sale of surveillance tools? And how can privacy be protected when data moves across the world in seconds?

PART 1, THE TOPIC: HARMS AND SOLUTIONS

Section 1A: The Harms

The people most directly harmed are those whom governments want to silence: journalists, activists, lawyers, opposition figures and their families. A much larger group, ordinary internet users, is harmed less dramatically but in far greater numbers, through data collection they cannot see or control.

1. United Nations Human Rights Office (A/HRC/51/17), August 4, 2022

Tagline: Counting the victims of Pegasus

Source: According to... United Nations Human Rights Office (Report A/HRC/51/17), August 4, 2022

Link: <https://docs.un.org/en/A/HRC/51/17>

Fact: It states... a leaked list of more than 50,000 phone numbers of possible surveillance targets, together with forensic checks of infected phones, showed that at least 189 journalists, 85 human rights defenders and more than 600 politicians and government officials were targeted with the Pegasus spyware. Judges, lawyers, doctors, union leaders and academics were also spied on. The company that makes Pegasus, NSO Group, admitted its customers target 12,000 to 13,000 people each year.

This means... the harm is not imaginary or small: a single company's product reached thousands of people, many of whom are the voices a democracy depends on. Delegates must decide whether the company, the buying government, or both should answer for this.

2. United Nations Human Rights Office (A/HRC/51/17), August 4, 2022

Tagline: Measuring the size of the spyware market

Source: According to... United Nations Human Rights Office (Report A/HRC/51/17), August 4, 2022

Link: <https://docs.un.org/en/A/HRC/51/17>

Fact: It states... Pegasus is only the most famous example. Researchers found that at least 65 governments had acquired commercial spyware, NSO alone reported 60 government agencies in 45 countries as customers, and more than 500 companies reportedly develop and sell surveillance tools to governments. In 2021, Meta disabled seven surveillance-for-hire firms that had targeted people in more than 100 countries and warned about 50,000 users.

This means... the problem is an industry, not a single harmful company. A resolution that targets only one firm will likely leave hundreds of others untouched.

3. Carnegie Endowment for International Peace, March 14, 2023

Tagline: Mapping which governments buy spyware

Source: According to... Carnegie Endowment for International Peace, March 14, 2023

Link: <https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses>

Fact: It states... at least 74 governments bought commercial spyware or digital forensics tools between 2011 and 2023. Of these, 44 were autocracies and 30 were democracies, and 56 of the 74 bought from firms based in or connected to Israel. More than 2,000 United States law enforcement agencies have also bought phone-extraction tools.

This means... both autocracies and democracies are customers, so no bloc can claim clean hands. This shapes coalition-building: a delegate who demands strict limits may find that their own government is a buyer.

4. Atlantic Council, September 4, 2024

Tagline: Tracing the companies behind spyware

Source: According to... Atlantic Council, September 4, 2024

Link: <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/>

Fact: It states... researchers mapped 435 entities in 42 countries connected to the spyware market, including 49 vendors, 36 subsidiaries, 32 holding companies and 95 investors. Most are based in Israel, Italy and India. Vendors often change names and move their corporate structures between countries, and cross-border investment money keeps the market growing.

This means... accountability is hard because firms can simply rename themselves or move to a country with weaker rules. Delegates may want solutions that follow the money (investors) and the people (founders), not just a company's current name.

5. Atlantic Council, September 10, 2025

Tagline: Following new money into spyware

Source: According to... Atlantic Council, September 10, 2025

Link: <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/>

Fact: It states... an updated map of the spyware market now covers 561 entities in 46 countries, adding 130 entities, 43 of them created in 2024. The number of investors based in the United States rose from 11 to 31, making the United States the largest investor country in the sample, even though some of the firms they fund are on the United States Entity List (a list of companies that face trade restrictions). Resellers and brokers, the middlemen who connect vendors to new buyers, are an important and poorly studied part of the market; Mexico alone had ten.

This means... the market kept growing after the first study, and money from a country that officially opposes spyware abuse helps fund it. Delegates can propose rules that cover investors and brokers, not only the companies that write the software.

6. Google Threat Analysis Group, February 6, 2024

Tagline: Linking vendors to zero-day attacks

Source: According to... Google Threat Analysis Group, February 6, 2024

Link: <https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/>

Fact: It states... commercial surveillance vendors are behind roughly half of the known zero-day exploits (attacks using secret, unpatched software flaws) aimed at Google products and Android devices. Google actively tracks about 40 such vendors, and dozens of smaller firms also play a role.

This means... spyware companies do not only harm their targets; by hoarding secret software flaws, they make everyone's phone less safe. This gives delegates a security argument, not just a human rights argument, for regulating the industry.

7. Citizen Lab (University of Toronto), March 19, 2025

Tagline: Exposing a newer spyware vendor

Source: According to... Citizen Lab (University of Toronto), March 19, 2025

Link: <https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/>

Fact: It states... Paragon Solutions, an Israeli firm founded in 2019 that sells the Graphite spyware and claims to avoid the abuses linked to NSO Group, appears to have deployments in Australia, Canada, Cyprus, Denmark, Israel and Singapore, and Italy is an acknowledged customer. In January 2025, WhatsApp warned about 90 accounts, including journalists and members of civil society, that they had been targeted.

This means... even a vendor that markets itself as "responsible" and sells mainly to democracies has been linked to targeting journalists. Voluntary company promises may not be enough on their own.

8. Citizen Lab (University of Toronto), June 12, 2025

Tagline: Confirming spyware on journalists' phones

Source: According to... Citizen Lab (University of Toronto), June 12, 2025

Link: <https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/>

Fact: It states... forensic analysis confirmed that the iPhones of two journalists, including Ciro Pellegrino of the Italian news site Fanpage.it, were attacked with Paragon's Graphite spyware in early 2025 through a zero-click attack that Apple later fixed. Both attacks traced back to the same Paragon customer. On June 5, 2025, an Italian parliamentary committee (COPASIR) acknowledged that the government had used Graphite against two activists, but could not say who targeted the editor of Fanpage.it.

This means... spyware abuse is not limited to authoritarian states; it has reached journalists inside the European Union. Delegates can argue that democracies that buy spyware also need outside oversight.

9. UN Special Rapporteur on Freedom of Expression (A/HRC/41/35), May 28, 2019

Tagline: Connecting surveillance to detention and torture

Source: According to... UN Special Rapporteur on Freedom of Expression (Report A/HRC/41/35), May 28, 2019

Link: <https://docs.un.org/en/A/HRC/41/35>

Fact: It states... surveillance of journalists, activists, opposition figures and critics has been shown to lead to arbitrary detention, sometimes torture and possibly killings outside the law. The report says this surveillance has grown because controls on selling technology to repressive governments are weak.

This means... the most severe harm is physical, not just a loss of privacy. Delegates arguing for strong rules can point out that surveillance is often the first step before arrest or violence.

10. United Nations Human Rights Office (A/HRC/51/17), August 4, 2022

Tagline: Watching public spaces through cameras

Source: According to... United Nations Human Rights Office (Report A/HRC/51/17), August 4, 2022

Link: <https://docs.un.org/en/A/HRC/51/17>

Fact: It states... the number of surveillance cameras in use worldwide was expected to pass one billion in 2021. Cameras with built-in video analysis grew from under 2 percent of network cameras sold in 2010 to over 40 percent by 2016, increasingly with facial recognition. Some companies build private camera systems that report to authorities or give them direct access, which expands surveillance while reducing oversight.

This means... corporate surveillance is not only spyware aimed at a few people; it is also mass monitoring of streets, shops and protests. Delegates must decide whether public-space surveillance by private companies needs separate rules.

11. United Nations Human Rights Office (A/HRC/48/31), September 13, 2021

Tagline: Explaining how data brokers operate

Source: According to... United Nations Human Rights Office (Report A/HRC/48/31), September 13, 2021

Link: <https://docs.un.org/en/A/HRC/48/31>

Fact: It states... many businesses design their services to collect as much data as possible, and social media firms earn money from massive amounts of user data. Data brokers buy, combine, analyze and share personal data with countless buyers, and these deals are mostly hidden from public view and only lightly limited by law. Data breaches have repeatedly exposed the sensitive information of millions of people.

This means... the "everyday" side of this topic touches almost every internet user. Any SPECPOL resolution that ignores data brokers leaves a major route from company databases to government hands unaddressed.

12. Sanford School of Public Policy, Duke University, November 2023

Tagline: Buying soldiers' personal data cheaply

Source: According to... Sanford School of Public Policy, Duke University, November 2023

Link: <https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/>

Fact: It states... researchers bought sensitive, non-public data about active-duty United States military members, their families and veterans from data brokers, including health, financial and religious information, for as little as 12 cents per record. Brokers checked buyers' identities inconsistently, including for buyers outside the United States, and the authors describe the industry as "highly unregulated." They warn that foreign or criminal actors could use such data to profile, blackmail or target people.

This means... the data economy is a security problem, not only a privacy problem: almost anyone, including a foreign government, may be able to buy sensitive data. Delegates from very different blocs can support limits on selling personal data across borders.

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

Tagline: Showing who is harmed most

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... the harm from data collection falls hardest on people whose information concerns gender identity, sexuality, location or health. Health apps may hold data reachable by police where some medical care is a crime, dating apps have been used to investigate and prosecute LGBTQI+ people, and insurers that buy data from data brokers may deny coverage based on health or even possible future health.

This means... privacy harms are unequal: groups already at risk suffer the most. Delegates can argue that protecting sensitive data is a question of discrimination, not just convenience.

14. Pew Research Center, October 18, 2023

Tagline: Measuring public distrust of companies

Source: According to... Pew Research Center, October 18, 2023

Link: <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>

Fact: It states... in a survey of 5,101 American adults, 67 percent said they understand little or nothing about what companies do with their data, 73 percent said they have little or no control over it, and 77 percent had little or no trust that social media leaders will admit mistakes about data misuse. Among those who had heard of AI, 81 percent expected it to lead to personal information being used in uncomfortable ways.

This means... even in a country that is home to many of the largest tech firms, most people feel powerless over their data. Delegates can use this to show that public support for stronger accountability rules exists.

15. The Guardian, September 3, 2026

Tagline: Recording Serbia's largest wave of spyware attacks

Source: According to... The Guardian, September 3, 2026

Link: <https://www.theguardian.com/world/2026/sep/03/serbians-targeted-with-advanced-spyware>

Fact: It states... at least 14 people from Serbian civil society, including members of a large student protest movement, were targeted with advanced spyware earlier in 2026. The digital rights group Share Foundation called it the largest documented wave of surveillance in Serbia so far. The attacks came to light in August 2026, when Apple warned users in 110 countries that they had probably been targeted by mercenary spyware. NSO Group, the maker of Pegasus, is now under United States ownership and is trying to get off a United States Commerce Department blacklist.

This means... spyware is still being used against peaceful protesters in 2026, shortly before national elections. Warnings that reached people in 110 countries show the problem is worldwide, and NSO's change of owner shows that a company can change hands without changing what its product does.

16. Citizen Lab (University of Toronto), July 3, 2026

Tagline: Hacking a lawmaker who investigated spyware

Source: According to... Citizen Lab (University of Toronto), July 3, 2026

Link: <https://citizenlab.ca/research/member-of-committee-investigating-spyware-hacked-with-pegasus/>

Fact: It states... forensic analysis found with high confidence that the iPhone of Stelios Kouloglou, a former Member of the European Parliament, was infected with Pegasus on or around October 21, 2022, and again on March 6 and 7, 2023. At that time he sat on the PEGA committee, the European Parliament's inquiry into spyware abuse, so the attackers could have reached confidential committee documents and discussions. He received Apple threat warnings on three occasions, but such warnings often arrive months after an attack.

This means... spyware has been aimed even at the lawmakers whose job is to investigate it. Delegates can argue that oversight bodies need protection of their own, or the people meant to hold spyware users to account can themselves be watched.

17. PBS NewsHour (Associated Press), March 23, 2026

Tagline: Turning street cameras into a weapon

Source: According to... PBS NewsHour (Associated Press), March 23, 2026

Link: <https://www.pbs.org/newshour/world/iran-built-a-vast-camera-network-to-control-dissent-israel-used-it-to-track-targets-ap-sources-say>

Fact: It states... hundreds of millions of internet-connected cameras, many of them poorly secured, are installed around the world. According to an intelligence official and another person briefed on the operation, Israel used hacked street cameras in Tehran, together with other intelligence, to help track Iran's supreme leader, Ayatollah Ali Khamenei, before he was killed on February 28, 2026. Iran had installed tens of thousands of cameras in its capital in response to protests. A security engineer told AP that a 2026 scan found nearly three million unprotected camera feeds in almost every country.

This means... camera networks that companies sell to watch citizens can be turned against the very government that bought them. This gives every bloc, including states that rely on cameras for control, a security reason to demand higher safety standards from surveillance equipment makers.

18. Center for Strategic and International Studies (CSIS), September 16, 2026

Tagline: Combining stolen data with AI

Source: According to... Center for Strategic and International Studies (CSIS), September 16, 2026

Link: <https://www.csis.org/analysis/what-drivers-license-breach-shows-about-foreign-data-ai-threats>

Fact: It states... an identity theft service advertised scans of more than 153 million driver's licenses from the United States and Canada on the dark web. The analysis warns that a foreign government could join this data to records stolen in earlier hacks, such as personal information on more than 145 million Americans taken from the data broker Equifax and records on 22.1 million people taken from the United States Office of Personnel Management in 2015, and then use AI tools to build detailed files on almost anyone.

This means... every company database is a possible target, and AI makes old leaks more dangerous because separate leaks can be combined. Delegates can argue that companies holding personal data should carry security duties, not only privacy duties.

19. Brookings Institution, May 20, 2026

Tagline: Showing how governments buy company tools

Source: According to... Brookings Institution, May 20, 2026

Link: <https://www.brookings.edu/articles/ice-acquisition-of-surveillance-technologies-accelerates-the-loss-of-public-trust-in-dhs/>

Fact: It states... United States immigration enforcement (ICE) uses surveillance technology bought from companies, including facial recognition, automatic license plate readers, cell-site simulators (devices that pretend to be cell towers so they can locate nearby phones), phone location databases and digital forensic tools that break into phones and computers. Some of these tools were funded by a law passed in July 2025. The author argues that Congress has failed to regulate these technologies, so their misuse should come as no surprise.

This means... the line between corporate surveillance and government surveillance is thin, because governments often buy what companies build. Delegates can argue that rules must cover the buyer and the seller together, and that this applies to democracies as well as autocracies.

20. The Guardian, August 3, 2026

Tagline: Pressing a company to weaken encryption

Source: According to... The Guardian, August 3, 2026

Link: <https://www.theguardian.com/technology/2026/aug/03/apple-legal-challenge-uk-government-data-access>

Fact: It states... Apple launched a legal challenge at the Investigatory Powers Tribunal against a second United Kingdom government demand, made under the Investigatory Powers Act, for "back door" access to the encrypted iCloud data of British users. The United Kingdom had dropped an earlier demand, which also covered American users, after a dispute with Washington. Both Apple and the Home Office are legally barred from discussing these secret orders.

This means... governments do not only buy surveillance from companies; they can also order companies to weaken their own security. Delegates must decide whether a resolution should protect encryption against demands from democracies as well as from autocracies.

Section 1B: Major Potential Solutions

Solution 1: A Global Moratorium on Spyware Sales

A moratorium is a temporary stop. Under this solution, states would halt the sale, transfer and use of commercial spyware until strong human rights rules exist.

- **Advantages:** It is the fastest and simplest way to stop new abuses; it has strong backing from UN experts; it puts the burden on the industry to prove it can operate safely.
- **Disadvantages:** It is not legally binding unless written into a treaty; states that buy spyware for real security work will resist; buyers and sellers may simply move to jurisdictions that ignore it.

21. UN Human Rights Experts (OHCHR), August 12, 2021

Tagline: Demanding a global moratorium

Source: According to... United Nations Human Rights Office (OHCHR), August 12, 2021

Link: <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening>

Fact: It states... UN human rights experts said letting the surveillance trade operate as a "human rights-free zone" is highly dangerous, and called on all states to impose a global moratorium on selling and transferring surveillance technology until strong rules are in place. They noted that a UN Special Rapporteur had called for a moratorium two years earlier, and the international community did not act.

This means... a moratorium has the UN's own experts behind it, which gives delegates authority to cite. It also shows the core weakness: calls for a pause have so far been ignored.

22. Carnegie Endowment for International Peace, March 14, 2023

Tagline: Warning that buyers switch suppliers

Source: According to... Carnegie Endowment for International Peace, March 14, 2023

Link: <https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses>

Fact: It states... the spyware market is resilient: when major vendors such as FinFisher and Hacking Team faded, buyers moved to newer suppliers, and penalizing one firm does little to reduce overall demand. Smaller boutique firms and open-source malware make attacks cheaper and harder to trace.

This means... a moratorium or sanction that only some countries respect may just shift business elsewhere. Delegates who support a moratorium must explain how to make it universal, or how to reduce demand from governments.

Solution 2: Stronger Export Controls on Surveillance Technology

Export controls require a government license before a company can sell certain products abroad. This solution would add human rights checks to those licenses.

- **Advantages:** It uses systems that already exist in many countries; it targets sales to governments known for abuse; it lets legitimate security trade continue.
- **Disadvantages:** The main international export arrangement is voluntary and was designed for military security, not human rights; enforcement is uneven; major producer countries are not all members.

23. United Nations Human Rights Office (OHCHR press release), September 16, 2022

Tagline: Calling for export control regimes

Source: According to... United Nations Human Rights Office (OHCHR), September 16, 2022

Link: <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>

Fact: It states... the UN Human Rights Office called on all states to immediately set up strong export control regimes for surveillance technologies that pose serious human rights risks, to assess the human rights situation in the country receiving the tools, and to use device hacking only as a last resort for a specific serious crime or threat. It also repeated the call for a moratorium on hacking tools.

This means... export controls are the UN's preferred "practical" step that most countries could adopt quickly. A SPECPOL resolution can call for them without needing a new treaty.

24. UN Special Rapporteur on Freedom of Expression (A/HRC/41/35), May 28, 2019

Tagline: Showing the limits of Wassenaar

Source: According to... UN Special Rapporteur on Freedom of Expression (Report A/HRC/41/35), May 28, 2019

Link: <https://docs.un.org/en/A/HRC/41/35>

Fact: It states... the main international export control regime, the non-binding Wassenaar Arrangement of 42 states, was built to reduce military threats and lacks guidelines or enforcement on human rights. It added "intrusion software" to its control list in 2013, but reported abuses show it has not meaningfully limited the spread of surveillance tools to repressive users.

This means... simply asking states to follow existing export rules has already been tried and has not worked well. Delegates may need to propose a human rights test inside export rules, or a new body to enforce them.

Solution 3: A Binding Treaty on Business and Human Rights

This solution would create a legally binding international treaty that makes companies, including tech and surveillance firms, legally responsible for human rights harms and gives victims a path to compensation.

- **Advantages:** It turns voluntary principles into law; it gives victims access to courts across borders; it closes the gap that lets firms move to weak jurisdictions.
- **Disadvantages:** Negotiations have taken over a decade with no final text; many wealthy home countries of large companies opposed the process at the start; a treaty only binds states that join.

25. United Nations Human Rights Council (A/HRC/RES/26/9), July 14, 2014

Tagline: Launching the binding treaty process

Source: According to... United Nations Human Rights Council (Resolution A/HRC/RES/26/9), July 14, 2014

Link: <https://docs.un.org/en/A/HRC/RES/26/9>

Fact: It states... the Council created an intergovernmental working group to write a legally binding international instrument regulating the human rights impact of transnational corporations and other businesses. The vote was 20 in favour, 14 against and 13 abstentions; those against included France, Germany, Japan, the Republic of Korea, the United Kingdom and the United States.

This means... the split vote shows a real political divide: many states whose companies dominate tech opposed binding rules. Delegates should expect this divide to appear in SPECPOL as well.

26. United Nations Human Rights Office (OEIGWG page), Last Accessed: October 2026

Tagline: Tracking slow treaty negotiations

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

Link: <https://www.ohchr.org/en/hr-bodies/hrc/wg-trans-corp/igwg-on-tnc>

Fact: It states... the working group has held eleven sessions, the latest in 2025, and is still negotiating an "updated draft legally binding instrument." The twelfth session is scheduled for October 12-16, 2026.

This means... the treaty is live and could be referenced in December 2026, but after twelve years it is still not finished. Delegates can propose to support or speed up this process rather than invent a new one.

Solution 4: Comprehensive Data Protection Laws Everywhere

This solution asks every country to adopt strong data protection laws, ideally based on shared international standards, and asks companies to follow clear rules on consent, data minimization and transparency.

- **Advantages:** It protects ordinary users, not only high-profile targets; it reduces the data available for abuse; it builds on laws most countries already have.
- **Disadvantages:** Many developing countries lack the money and experts to enforce such laws; standards differ between regions; national security exceptions can empty the rules of meaning.

27. UN Trade and Development (UNCTAD), Last Accessed: October 2026

Tagline: Counting countries with privacy laws

Source: According to... UN Trade and Development (UNCTAD), Last Accessed: October 2026

Link: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

Fact: It states... 137 of 194 countries have put in place legislation to protect data and privacy.

This means... about 57 countries still have no such law, and those are often where companies can collect data with the fewest limits. Capacity-building for these countries is a realistic resolution clause.

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

Tagline: Listing what companies must do

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 called on all businesses that collect and process data to review their business models against the UN Guiding Principles on Business and Human Rights, inform users clearly about data collection, avoid collecting data without consent or a legal basis, let people access, correct and delete their data, and add safeguards that prevent misuse of their products, including notifying relevant parties when misuse is detected.

This means... the UN has already written a detailed checklist for companies, but these are calls, not legal duties. Delegates can debate whether to turn this list into binding obligations or a reporting system.

Solution 5: Banning the Most Dangerous AI Surveillance Uses

This solution would ban or pause specific uses of AI that cannot respect human rights, such as real-time facial recognition in public spaces or scraping photos from the internet to build face databases.

- **Advantages:** It is precise, targeting the highest-risk uses; at least one major region has already done it; it pushes companies to design with rights in mind.
- **Disadvantages:** Bans often exempt national security and policing; definitions can be avoided by changing a product slightly; countries with large AI industries may see bans as limiting innovation.

29. United Nations Human Rights Office (A/HRC/48/31), September 13, 2021

Tagline: Recommending bans and moratoriums

Source: According to... United Nations Human Rights Office (Report A/HRC/48/31), September 13, 2021

Link: <https://docs.un.org/en/A/HRC/48/31>

Fact: It states... the High Commissioner recommended that states expressly ban AI applications that cannot be operated in line with international human rights law, place moratoriums on selling and using high-risk AI systems until safeguards exist, and impose a moratorium on remote biometric recognition in public spaces.

This means... the UN Human Rights Office already supports targeted bans, so delegates proposing them are within the UN's own recommendations.

30. European Commission, August 3, 2026

Tagline: Showing a regional ban in action

Source: According to... European Commission, August 3, 2026

Link: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Fact: It states... the European Union's AI Act, in force since August 1, 2024, has banned since February 2, 2025 several practices including untargeted scraping of internet or camera images to build facial recognition databases, real-time remote biometric identification for policing in public spaces, and emotion recognition in workplaces and schools. Stricter "high-risk" rules for remote biometric identification will apply from December 2, 2027. Under a 2026 simplification law known as the "AI Omnibus," which entered into force on July 27, 2026, a ninth ban, on AI apps that create non-consensual sexual images, takes effect in December 2026.

This means... bans are not only theory; a group of 27 states is already enforcing them. Delegates can cite this as a working model, while noting that it binds only EU members and the companies selling into the EU.

31. The Guardian, September 29, 2026

Tagline: Testing facial recognition in train stations

Source: According to... The Guardian, September 29, 2026

Link: <https://www.theguardian.com/technology/2026/sep/29/trial-live-facial-recognition-cameras-london-stations-false-positive>

Fact: It states... a six-month trial of live facial recognition by British Transport Police in London railway stations, from February to July 2026, scanned more than half a million faces, cost more than 320,000 pounds and used almost 100 hours of police time. It produced only one alert, which was an incorrect identification, and no arrests. Police have since extended the trial for four more months and added London Underground stations.

This means... mass face scanning can cost a great deal and catch very few people, while scanning everyone who walks past. Delegates who support bans can use this to question whether the benefits justify the privacy cost; delegates who oppose bans can point out that the police chose to continue and expand the trial.

32. The Guardian, October 5, 2026

Tagline: Pausing smart glasses in public places

Source: According to... The Guardian, October 5, 2026

Link: <https://www.theguardian.com/world/2026/oct/05/norway-temporary-ban-smart-glasses-public-places>

Fact: It states... Norway plans a temporary ban on camera-enabled smart glasses in places such as parks, beaches, museums, shopping centres, schools, healthcare facilities and public events, while an expert group writes permanent rules. Norway's minister of digital affairs said people risk being photographed, filmed or recorded without knowing it. Meta has sold at least 9 million pairs of its Ray-Ban smart glasses since the start of 2023.

This means... new consumer devices are carrying recording into everyday places faster than laws can follow. A temporary ban while permanent rules are written is a model delegates can borrow, because it is a pause rather than a permanent prohibition.

Section 1C: Lesser Solutions (brief list)

- **Protecting encryption:** Ask states not to require "backdoors" or scanning of private messages, as the UN Human Rights Office recommended in 2022 (see entry 23).
- **Digital literacy:** Fund education so citizens understand how their data is used; the General Assembly encouraged this in A/RES/79/175, paragraph 13.
- **Investor scrutiny:** Ask investment funds to check whether they finance spyware vendors, following the Atlantic Council's finding that 95 investors sit inside the market (see entry 4).
- **Victim notification:** Encourage platforms to warn users who are targeted, as Meta and WhatsApp have done (see entries 2 and 7).
- **Shared registries of surveillance firms:** Create public lists of vendors and their owners so firms cannot hide by renaming, as Carnegie recommended (see entry 3).
- **Remedy funds:** Create a way for victims in poorer countries to seek compensation when foreign companies' products are used against them.

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 Nougères 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/>

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.
-