

HMDC Presents... SPECPOL: Part 1 (The Topic)

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.

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 LGBTIQI+ 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.