

HMDC Presents... SPECPOL: Video 2 Transcripts

These are the words spoken in the two Video 2 films for SPECPOL (The United Nations and International Efforts). We read along while we watch, pause at each time mark, and circle any word we do not know so we can look it up together.

VIDEO 2 (EXPLAINER)

[0:00] Welcome, delegates. Let's jump right into this explainer. Today we're unpacking a massive issue for your upcoming SPECPOL Committee debate, corporate surveillance, accountability, and privacy. We're going to look at exactly what the United Nations and the rest of the world have actually done about this. So let's get started. Here's our roadmap for today. We're covering, one, the Human Rights Foundation, two, corporate rules and treaties, three, the Digital Privacy Agenda, four, assessing the UN record, five, international efforts and gaps, and finally, six, trends and future opportunities. Section one, the Human Rights Foundation, the bedrock of international law. Okay, to build a strong argument, you need the legal bedrock. According to a United Nations publication last accessed in October 2026, General Assembly Resolution A-R-E-S-2-17-A, Roman numeral three, adopted the Universal Declaration of Human Rights back in 1948. That established privacy protection in Article 12. Then, as noted by the United Nations Human Rights Office, also last accessed in October 2026, Resolution A-R-E-S-2200-A, Roman numeral 21, adopted the International Covenant on Civil and Political Rights in 1966.

[1:15] That is what made privacy a binding treaty right under Article 17. These two documents are literally the foundation of everything we're talking about today. Moving right along to section two, corporate rules and treaties, regulating business. Let's define two absolutely crucial terms you'll need to know. First up, guiding principles. Basically, these are voluntary corporate rules. It means companies are encouraged to follow them, but they aren't forced to do so by international law. On the flip side, we have a binding treaty. This is a legally enforced international agreement. If a country signs it, they have a strict legal duty to obey those rules. Knowing the difference between voluntary and binding is super important here. So, let's compare these two ideas in the real world. According to the United Nations Human Rights Council, on July 6, 2011, Resolution A-H-R-C-R-E-S-7-4 [Our report says: A/HRC/RES/17/4] created voluntary rules for companies, known as the guiding principles. Then, on July 14, 2014, the council passed Resolution A-H-R-C-R-E-S-26-9, which kicked off the process for an actual binding treaty.

[2:24] But there's a catch. That resolution faced a heavily split vote. The result? Highly undesirable slow progress, with no final text finished even after more than a decade of negotiations. All right, section three, the digital privacy agenda, the UN modernizes. To make sure we're all on the same page, let's clearly define three technical terms before we look at the timeline. Special Rapporteur is an independent UN expert whose job is to investigate a specific human rights theme, like privacy. Next, the global digital compact is a high-level international commitment made by world leaders about data and technology. And finally, the cyber crime convention is a new UN treaty specifically focused on investigating digital crimes across borders. Let's trace how the UN modernized this agenda. According to the United Nations Digital Library, on January 21, 2014, Resolution A-R-E-S-68-167 was actually adopted without a vote back in 2013, starting this whole process. This led to creating the Special Rapporteur on Privacy in 2015, a role that was just renewed in March 2024. Fast forward to late 2024, and the United Nations General Assembly made a huge push. On September 22, Resolution A-R-E-S-79-1 adopted the global digital compact. On December 17, Resolution A-R-E-S-79-175 officially named the private surveillance industry. Then, on December 24, Resolution A-R-E-S-79-243 adopted the cybercrime convention. And according to the UN Office on Drugs and Crime, last accessed in October 2026, that cybercrime convention was officially open for signature in Hanoi on October 25, 2025. Now for Section 4, Assessing the UN Record. What works and what does not?

[4:14] Before we judge these outcomes, we need one more definition, moratorium. A moratorium is just a temporary stop or a pause on a specific activity. You're going to hear this word a lot in committee, mostly from people debating whether we should place a moratorium on spyware sales until we have better rules. So, what's actually working? Well, we have some very helpful and desirable outcomes. We've got agreed language, detailed reports, and a dedicated privacy expert. But we also have to look at the harmful and undesirable realities. There are still zero binding duties on companies. And those calls for a moratorium? Totally ignored. For instance, according to the United Nations Human Rights Office on August 12, 2021, UN experts called for a pause on spyware sales. But the world just didn't act. On top of that, vital work is getting stalled. The United Nations Human Rights Office noted on August 29, 2025, that a major privacy report was delayed simply because of a UN cash crisis. That is definitely an undesirable situation. Next up, Section 5, International Efforts and Gaps. Beyond the UN. Let's clearly define two tools that are heavily regulated outside the UN. Export controls are strict government licenses. Basically, a company has to get legal permission before they can sell certain products to other countries. And spyware is the actual software we're talking about, the programs that get secretly installed on your phone or computer to track you without you ever knowing.

[5:40] Stepping outside the UN, it's really a patchwork of different efforts. For example, according to the Council of Europe, last accessed in October 2026, they created Convention 108 for data protection, along with a global AI treaty. Though that treaty does have an exemption for national security. Over in Europe, the European Commission, also accessed in October 2026, enforces its own export rules based on human rights. Taking a different angle, the OECD reached an agreement on limits to government data access in December 2022. And then you have the Government of the United Kingdom, which established the Pall Mall Process on April 4, 2025. That created a voluntary code for countries buying commercial cyber tools. One of the biggest mechanisms out there is the Wassenaar Arrangement, which controls the export of dual-use technology. According to the Wassenaar Arrangement website accessed in October 2026, it involves 42 participating states.

[6:31] But here's the catch. They rely on a strict consensus rule, meaning every single state has to agree to make a change. When you're dealing with fast-moving surveillance tech, that consensus rule creates highly undesirable limits on enforcement. We also have the Freedom Online Coalition. According to their records, accessed in October 2026, they unite 41 member governments trying to protect human rights online. But despite all these coalitions, the threat is everywhere. A report published by Citizen Lab on September 18, 2018 detected harmful spyware operations in 45 different countries. It really highlights how much we rely on independent researchers to expose these things. Finally, Section 6. Trends and Future Opportunities. The Delegates Challenge. The data paints a pretty stark picture for us. According to Freedom House, last accessed in October 2026, global internet freedom has declined for the 14th year in a row. That is a deeply undesirable trend, right? It proves that all these voluntary measures and fragmented international efforts just aren't cutting it when it comes to protecting human rights globally.

[7:36] So, delegates, I want to leave you with this provocative question. As you sit down to draft your resolutions, ask yourselves, what is the specific gap that the United Nations can fill that absolutely no one else can? Is it enforcing binding rules? Is it setting a universal standard? Your answer to that question is going to be the absolute foundation of your committee debate. Good luck.

VIDEO 2 (CINEMATIC)

[0:00] For over a decade, the United Nations has debated the rise of commercial spyware and massive corporate data collection. To understand how to regulate this threat, we have to look at what the international community has actually managed to accomplish. Digital privacy is often treated as a modern problem, but the core right is nearly 80 years old. In 1948, the UN Universal Declaration of Human Rights established that no one should face arbitrary interference with their privacy. That principle was written long before vendors began selling zero-click hacking tools capable of silently extracting every message, photo, and location point from a target smartphone. To give that principle legal weight, the UN adopted the International Covenant on Civil and Political Rights in 1966.

[0:45] Article 17 transformed privacy from a shared ideal into a binding treaty right. Nations that joined this treaty committed to providing legal protection against unlawful interference with a person's private life or correspondence. This mandate applies equally to state and commercial actors. Governments must restrain their own intelligence agencies, and they carry a binding legal duty to regulate the private companies operating within their borders. The foundation is already built. The widespread abuse of commercial surveillance tools today represents a failure to enforce existing law rather than a lack of legal definition. When it comes to managing corporate tech actors specifically, the UN relies heavily on the 2011 guiding principles on business and human rights. This framework rests on three pillars—the state's duty to protect, the corporate responsibility to respect, and the victim's access to remedy.

[1:36] However, these pillars carry no legal teeth. They depend entirely on a technology company choosing to voluntarily comply with human rights standards. Because these agreements lack enforcement mechanisms, they generate an illusion of momentum. Broad resolutions affirming the right to privacy in the digital age regularly pass the General Assembly by full consensus. But that consensus shatters the moment the UN attempts to create binding corporate law. When the Human Rights Council voted in 2014 to start drafting a legally binding treaty on transnational corporations, the chamber fractured. Wealthy states that host the majority of the world's largest technology companies systematically voted against the measure, preferring voluntary guidelines over mandatory international regulation.

[2:24] That diplomatic friction has stalled the process for over a decade. After 12 sessions, negotiators have yet to produce a final agreed-upon treaty text. Despite the gridlock on enforcement, the UN has made recent progress in diagnosing the exact source of the harm. In 2024, the General Assembly passed a resolution explicitly naming and expressing deep concern over the tools developed by the private surveillance industry. Isolating this specific industry forces the diplomatic conversation to shift away from theoretical debates about digital rights and toward targeted regulations on the companies building hacking tools. The United Nations has successfully diagnosed the commercial spyware threat, but it currently lacks the binding infrastructure to actually regulate the companies producing it.

[3:11] We can see the limits of international consensus in the UN's newest framework for cross-border data surveillance, the Cybercrime Convention, which opened for signature in late 2025. The treaty requires member states to apply human rights safeguards when sharing digital evidence, but it leaves the definition and enforcement of those safeguards up to each participating state's domestic laws. Consequently, if an autocratic government with weak domestic privacy protections requests user data, the treaty provides few international barriers to prevent that information from being handed over. This dynamic creates an accountability paradox. The UN possesses the world's leading experts and reporting capabilities, but it holds zero mechanisms to enforce its own findings. The institution successfully produces expert mandates, unifies diplomatic language, and executes granular, data-driven investigations into human rights abuses.

[4:06] Yet, when those very experts formally call for an immediate global moratorium on the sale of spyware, member states simply ignore the directive. Furthermore, the UN's internal liquidity crisis has forced the delay of critical privacy reports, actively stalling the organization's ability to maintain accountability. Because the UN cannot command compliance, the burden of regulation falls onto a fragmented ecosystem of external regional pacts, attempting to fill the global enforcement void. Europe has led the attempt to establish binding regional governance, drafting treaties like Convention 108 for data protection, and the 2024 Framework Convention on AI. These agreements enforce strict rules on commercial data processing, but they routinely grant broad, blanket exemptions for activities related to national security.

[4:57] Commercial spyware vendors exploit this exact loophole. By marketing their tools exclusively to military and law enforcement agencies, they bypass standard corporate data regulations. To close this gap, the European Union updated its dual-use export rules, allowing member states to block the physical sale of surveillance tech to governments with poor human rights records. Outside of Europe, the primary global system for tracking these exports is the Wassenaar Arrangement, a coordination pact among 42 participating states. Wassenaar is built to track conventional military hardware, not assess human rights. Compliance is voluntary, and updating the control list requires full consensus, meaning a single state can block any restriction on a surveillance vendor. Seeking an alternative, the United Kingdom and France launched the Pall Mall Process, organizing summits to draft a voluntary code of practice specifically for states that purchase commercial spyware.

[5:53] While highly targeted, this initiative remains an exclusive, non-binding coalition of mostly Western democracies, conspicuously lacking participation from the major buyers in the global south. Similarly, the Freedom Online Coalition unites dozens of governments to advocate for digital rights, but functions strictly as a voluntary bloc without legislative authority. The result is a global regulatory ecosystem that functions less as a safety net, and more as a patchwork of voluntary codes and regional loopholes, which commercial vendors easily navigate and bypass. This regulatory void leaves the actual tracking of digital abuses entirely to the private sector. Independent university researchers, rather than sovereign states or international treaties, are the entities exposing commercial spyware operations.

[6:44] Their forensics reveal that single spyware variants frequently infiltrate devices across dozens of countries simultaneously, proving that corporate surveillance effortlessly breaches physical national borders. This chart measures the global macroeconomic result of the policy gap, a consistent, documented decline in worldwide internet freedoms over more than a decade. The metrics show that digital liberties have steadily eroded for 14 consecutive years. This sustained erosion correlates directly with the international community's reliance on voluntary corporate guidelines and indefinitely stalled treaties. The empirical data proves that current diplomatic solutions are failing to halt or reverse the expansion of corporate surveillance. For the delegates of the Special Political and Decolonization Committee, this reality sets the specific mandate for the 2026 conference.

[7:36] The task is no longer to draft resolutions that simply restate rights established in 1948. The task is to build actionable enforcement mechanisms that hold private entities accountable across sovereign lines. You must determine exactly which governance gap, whether it is mandating human rights tests in export controls, drafting binding tech regulations, or funding data capacity building. This committee will practically fill.