

HMDC Presents... SPECPOL: Video 1 Transcripts

These are the words spoken in the two Video 1 films for SPECPOL (The Topic). 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 1 (EXPLAINER)

[0:00] Welcome, delegates, to this explainer on corporate surveillance, accountability, and privacy. We're going to be speaking clearly and taking our time today because this is a complex, often hidden global issue. But by the end of our time together, you'll have the exact factual baseline you need to succeed in your upcoming debates for the Special Political and Decolonization Committee. Here is our roadmap for today. We'll cover what corporate surveillance means, the harm it causes targeted individuals, the massive size of the industry, the impact on everyone else, five major policy solutions, and finally, we'll wrap up with how to choose your stance. Let's dive into section one, what corporate surveillance means. To start, it's absolutely crucial that we all share the same vocabulary.

[0:46] Corporate surveillance basically has two faces. The first is the direct hacking face, which relies on spyware. Spyware is software that is secretly installed on a device. Since it's there, it lets someone else read your private messages, track your exact physical location, and even silently switch on your camera or microphone. Now, you might be wondering, how does that spyware actually get onto a phone? Well, it's often through something called a zero-click attack. This is exactly what it sounds like. It's a hack that infects a device without the owner clicking a single link. You literally don't have to do anything wrong to get infected, which makes it incredibly hard to prevent. The zero-day exploit. This is an attack that uses a secret flaw in the software that the maker, like Apple or Google, does not yet know about.

[1:32] Because the maker has had zero days to fix it, there is no patch available, leaving targets completely defenseless. Finally, the second face of corporate surveillance is the everyday data economy, which is powered by data brokers. A data broker is a company that secretly buys, combines, and sells personal information about people. They silently harvest the digital footprints we all leave behind online, usually without our knowledge or direct consent. Harm to targeted people. The scale of who is being targeted is pretty alarming. According to the United Nations Human Rights Office on August 4, 2022, just one type of spyware called Pegasus targeted at least 189 journalists, 85 human rights defenders, and over 600 politicians. Furthermore, the company making Pegasus admits its customers target between 12,000 and 13,000 people every single year.

[2:24] And the consequences for those people are absolutely devastating. According to a statement by the UN Special Rapporteur on freedom of expression on May 28, 2019, this surveillance of journalists, activists, and critics has led to arbitrary detention, sometimes torture, and possibly killings outside the law. So we're talking about severe physical harm here, not just a breach of digital privacy. Let's look at Section 3, the size of the industry. To really grasp this crisis, we have to understand the global market driving it. Who exactly is buying these tools? Well, according to data published by the Carnegie Endowment for International Peace on March 14, 2023, 74 governments bought commercial spyware over a 12-year period. And this includes 44 autocracies, but also 30 democracies, showing that this trade crosses all political lines.

[3:15] And the market supplying them is vast and evasive. According to research released by the Atlantic Council on September 4, 2024, there are 435 entities connected to the spyware market, spread across 42 different countries. Holding them accountable is incredibly difficult because these firms constantly rename themselves and move across borders. The collateral damage to our global tech infrastructure is also massive. According to an analysis by the Google Threat Analysis Group on February 6, 2024, commercial surveillance vendors are behind roughly half of all known zero-day exploits aimed at Google products and Android devices worldwide. Harm to everyone else. Beyond targeted hacking, this massive surveillance machine impacts the privacy of ordinary citizens globally. It is deeply woven into our public spaces.

[4:02] According to a report from the United Nations Human Rights Office on August 4, 2022, the number of active surveillance cameras worldwide was expected to pass a staggering 1 billion in 2021. In our private lives, the collection is practically invisible. According to the United Nations Human Rights Office on September 13, 2021, data brokers execute hidden deals to trade our personal information. And crucially, a later report by the same office on August 29, 2025 explicitly noted that this mass data collection harms vulnerable and marginalized groups the most. As a result of all these hidden practices, public trust is breaking down. According to survey data published by the Pew Research Center on October 18, 2023, 73% of United States adults feel they have little or no control over their own personal data.

[4:50] Five major policy solutions. This is the crucial part for your committee prep. We're going to evaluate five core policy responses to see if they are helpful, harmful, desirable, or undesirable. First is a global moratorium, or pause, on spyware sales. This approach is helpful because it is the absolute fastest way to stop new abuses, and it's backed by UN experts. But it can be viewed as harmful because unsupported bans simply shift business to newer, unrestricted suppliers, and past UN calls for pauses have basically been ignored. Solution two is stronger export controls. This is desirable as a practical first step because it forces a human rights test onto government export licenses. However, it is undesirable because existing international frameworks are entirely non-binding. They are structurally weak when it comes to enforcement.

[5:39] Solution three is a binding business and human rights treaty. Legally, this is helpful to close the loopholes that allow firms to escape oversight by moving across borders. But as a short-term fix, it proves harmful because negotiations for this have been stalled for over 12 years, and major states that host tech firms may refuse to join. Solution four is comprehensive global data protection laws. Selecting this is highly desirable because it protects ordinary people from hidden data brokers. Yet, it remains undesirable as a quick global fix. Because according to UN Trade and Development in October 2026, 57 out of 194 countries still completely lack these laws, and developing nations often lack the funds to properly enforce them. Finally, solution five is banning the most dangerous AI surveillance.

[6:27] This is a helpful strategy to pause high-risk uses, a concept actually proven by the European Union AI Act bans in effect since February 2nd, 2025, according to European Commission data from October 2026 [Our report says: August 3, 2026]. On the flip side, it's considered harmful by some because broad national security exemptions leave massive loopholes, and some states argue these bans cripple technological innovation. So delegates, as we wrap up this explainer, I want to leave you with one final critical question for your committee preparation. Looking at the geopolitical reality of your assigned nation, and weighing the advantages and disadvantages we just discussed, which solution would your country support, and why? Good luck in your debates.

VIDEO 1 (CINEMATIC)

[0:00] Welcome to the briefing. Today, we are examining corporate surveillance, accountability, and privacy. Imagine your device is compromised, your microphone activated, and your encrypted messages read, without you ever touching a malicious link or downloading a suspicious file. This is known as a zero-click attack. This represents the sharpest edge of the spyware industry. These are private companies that build and sell highly targeted precision hacking tools designed to crack individual devices for paying governments. The second face of corporate surveillance is the data economy. Here, everyday apps, platforms, and data brokers operate as a vast, invisible dragnet, constantly extracting, combining, and selling personal information on a massive scale.

[0:48] For international policymakers, both faces of this industry present the same urgent crisis. Because the speed of technological development easily outpaces international law, both the spyware industry and data brokers operate in what United Nations experts call a human rights-free zone. Whether a device is breached by mercenary spyware or a user's physical movements are tracked and sold by a data broker, individuals lose their autonomy. Because these systems operate globally and outpace domestic laws, bringing them under control requires an international response. The rules governing this digital privacy crisis are being debated right now on the floor of the United Nations. This chart illustrates the confirmed targets of a single commercial spyware tool called Pegasus. Forensic evidence reveals at least 189 journalists, 85 human rights defenders, and more than 600 politicians and government officials were targeted.

[1:42] The consequences of this digital breach are intensely physical. UN reports document that the surveillance of activists and critics frequently serves as the first step toward arbitrary detention, and in some cases, torture or killings outside the law. This map details the 74 governments, 44 autocracies and 30 democracies that purchased commercial spyware between 2011 and 2023. Accountability is difficult because the 435 entities in this market frequently rename themselves and move structures across international borders to avoid oversight. By exploiting vulnerabilities for profit, the spyware market makes the entire internet less safe for everyone. While their corporate shell games allow them to easily evade national jurisdiction.

[2:29] Beyond targeted political spyware, we must now shift our focus to examine the mass extraction of everyday citizens' personal data. In public spaces, the physical scale of modern monitoring is staggering. By 2021, the number of surveillance cameras worldwide was expected to pass 1 billion, increasingly equipped with facial recognition. This survey graphic measures public distrust in the data economy. It shows that 73% of surveyed adults report having little or no control over what companies do with their personal data. The surveillance industry also creates a systemic security threat. Commercial vendors actively hoard undisclosed software flaws known as zero-day exploits. In fact, they are behind roughly half of all known zero-day attacks aimed at major tech ecosystems like Google and Android.

[3:19] Whether a company is selling a mercenary hacking tool to a foreign government or harvesting massive databases of consumer behavior, the accountability gap remains identical. These corporations operate globally, while regulatory enforcement remains localized and weak. For delegates in the Special Political and Decolonization Committee, the task is to evaluate five distinct international frameworks designed to close this accountability gap. Solution 1 proposes a global moratorium, an immediate, temporary halt to the sale and transfer of commercial spyware. The primary vulnerability here is market resilience. Solution, when penalized, rogue buyers simply shift their business to newer, less regulated suppliers. Solution 2 focuses on stronger export controls. This would require governments to apply a strict human rights assessment to surveillance tools before issuing a license for them to cross borders.

[4:11] The structural flaw with current global export arrangements is that they operate entirely on consensus and lack meaningful enforcement mechanisms, leaving each participating state to decide on transfers independently. Solution 3 is drafting a binding international treaty on business and human rights. This shifts the framework from voluntary corporate guidelines into strict legal accountability, giving victims a clear path to compensation. The idealism of these legal interventions meets a harsh political reality. Negotiations for a binding treaty have faced intense division, with several major tech-producing nations historically voting against the process. Solution 4 takes a systemic approach, implementing comprehensive data protection laws everywhere. This requires every country to establish clear rules on consent and transparency to protect ordinary users from data brokers.

[5:01] This map highlights the current global adoption rate of privacy laws. While 137 countries have active legislation in place, roughly 57 nations are left entirely unprotected. Many developing countries currently lack the financial resources and technical experts required to enforce these laws. Solution 5 targets the most dangerous applications of technology through specific AI surveillance bans. This would pause practices like real-time facial recognition in public spaces. The European Union has already set a regional precedent by enforcing bans on untargeted biometric identification. Yet on a global scale, there is persistent pushback from states demanding broad exemptions for policing and national security. Policy makers are left with a core structural dilemma. They must decide if a single international framework can successfully regulate both the precision of mercenary spyware and the sheer breadth of corporate data extraction.

[5:57] The evidence is on the table. It is now up to the delegates to weigh these policy options and determine exactly which combination of mechanisms their country will champion in committee.