



LUSAKA OAKTREE SCHOOL MODEL UNITED NATIONS
LOTSMUN 2026

Architects of Accountability • Redefining Power, Peace and Progress

STUDY GUIDE

Human Rights Commission | High School

**Topic: State Surveillance, Biometric Data Tracking and the Proliferation
of Commercial Spyware**

Message from the Secretary General

Dear Delegates,

It is my great pleasure to welcome you to LOTSMUN 2026.

This year, under the theme “Architects of Accountability: Redefining Power, Peace and Progress,” we invite you to consider not only how decisions are made but who is responsible for them, who is affected by them and how meaningful change can be achieved.

Model United Nations is more than an exercise in public speaking. It is an opportunity to understand complex international problems, challenge assumptions, negotiate with people who may disagree with you and transform competing ideas into meaningful solutions.

As you prepare for this committee, I encourage you to look beyond the information presented in this study guide. The purpose of this document is not to provide you with every answer, but to provide you with the foundation from which your own research, perspectives, and ideas can develop.

Come prepared to question, collaborate, negotiate and most importantly, represent your country’s position with accuracy and diplomacy. Remember that accountability is not simply about holding power responsible; it is about understanding how power can be used to build peace, drive progress, and create meaningful change.

I look forward to seeing the ideas, debates, and solutions you bring into committee.

Malenji Arthur Jonah

Secretary General, LOTSMUN 2026

ZAMBIA MODEL UNITED NATIONS

1. The Human Rights Commission

1.1 What is this committee?

This committee is modelled on the United Nations' main human rights body. Strictly, the UN **Commission on Human Rights** was replaced in 2006 by the **Human Rights Council**, which meets at the UN Office in Geneva.¹ The Council has **47 member states**, elected by a majority of the 193 members of the UN General Assembly. Members serve three-year terms, and one-third of the seats are renewed each year.²

In this simulation, you are a **member state**. The Council cannot arrest anyone or force a government to act. Its resolutions send "a strong political signal which can prompt governments to take action".³ Here are the bodies and tools you are most likely to cite:

Body or tool	What it does
Human Rights Council	Debates human rights issues and adopts resolutions that express international consensus. ⁴
Universal Periodic Review (UPR)	Reviews the human rights record of every UN member state. ⁵
Special Procedures	Independent experts who monitor particular countries or themes. ⁶
Special Rapporteur on the right to privacy	Created by the Council on 26 March 2015 to focus on privacy in the digital age, gather information and make recommendations. ⁷
Office of the High Commissioner (OHCHR)	The UN human rights office. Its reports on privacy, spyware and biometrics are among the best sources for this topic. ^{8,9}
Universal Declaration of Human Rights	The 1948 declaration. Article 12 protects against arbitrary interference with privacy, Article 19 protects expression and Article 20 protects assembly. ¹⁰

¹ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council. <https://www.ohchr.org/en/hr-bodies/hrc/about-council>

² UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

³ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

⁴ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

⁵ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

⁶ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

⁷ OHCHR. Human Rights Council creates mandate of Special Rapporteur on the right to privacy (26 March 2015). <https://www.ohchr.org/en/press-releases/2015/03/human-rights-council-creates-mandate-special-rapporteur-right-privacy>

⁸ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns (press release, 16 September 2022). <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>

⁹ OHCHR. A/HRC/60/45: The right to privacy in the digital age (report of the High Commissioner, 29 August 2025). <https://www.ohchr.org/en/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high>

¹⁰ United Nations. Universal Declaration of Human Rights (adopted 10 December 1948). <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

2. Introduction to the Topic

This topic has three connected parts. **State surveillance** means governments monitoring people's communications, movements and online activity. **Biometric data tracking** means collecting and using body-based data, such as faces, fingerprints and irises, to identify people. **Commercial spyware** means hacking tools that private companies build and sell, often to governments, to take over phones and computers.

Here is one way the problem develops:



This is a simplified picture, and surveillance is sometimes lawful and useful. The UN human rights office says the key question is whether it is “strictly necessary and proportionate”, which this guide returns to below.¹¹

2.1 The scale of the problem

Spyware. The 2021 Pegasus Project investigation found more than **50,000 phone numbers** that NSO Group’s clients were believed to have selected as targets since 2016. They included more than **180 journalists**, and also business executives, academics, union officials and government officials. Amnesty International checked 67 suspected phones and found 23 were infected and 14 showed attempted infection.¹²

The UN view. The UN human rights office warns that tools like Pegasus can turn a smartphone into a “24-hour surveillance device”, and that governments often use them “to clamp down on critical or dissenting views”.¹³ It also says that digital identity systems and biometric databases have removed many of the practical limits that once restricted surveillance.¹⁴

50,000+ phone numbers on the Pegasus Project list (2021)	1,400 WhatsApp users infected by Pegasus, found by a US jury (2025)	25 governments signed the Pall Mall Code of Practice (2025)
--	---	---

Biometrics. In September 2021 the UN human rights office called on states to pause (a **moratorium**) the use of remote biometric recognition in public spaces until safeguards exist, and described real-time facial

¹¹ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

¹² Business and Human Rights Resource Centre. Investigation finds NSO Group spyware sold to governments used against activists, politicians and journalists; company denies allegations (Pegasus Project, July 2021). <https://www.business-humanrights.org/en/latest-news/nso-group-spyware-sold-to-governments-used-to-target-activists-politicians-journalists-according-to-pegasus-project-investigation-company-denies-allegations/>

¹³ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

¹⁴ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

recognition as especially threatening.¹⁵ A 2025 UN report also looks at how data collection can deepen discrimination and unequal privacy protection.¹⁶

2.2 The test for any surveillance measure

Human rights law does not ban all surveillance. It bans **arbitrary** interference with privacy.¹⁷ The ICCPR, a binding treaty for its parties, adds that interference must not be **unlawful** either.¹⁸ The UN human rights office says measures must be “strictly necessary and proportionate”, and that device intrusion should be a **last resort** for serious threats or crimes.¹⁹ Use this checklist (standard human rights practice):

Question	What it asks
Legal?	Is it based on a clear, public law, not secret orders or vague wording?
Necessary?	Is there a real aim, such as serious crime or national security, and no less intrusive way?
Proportionate?	Is the intrusion limited in scope, place and time, compared with the harm it prevents? ²⁰
Overseen?	Does a court or independent body authorise and review it? ²¹
Remedy?	Can a person find out, complain and receive redress if their rights were violated?

2.3 Ideas, tools and frameworks to know

Idea or tool	What it is
Moratorium	A temporary pause. The UN human rights office has urged one on spyware use and sales until safeguards exist, and on remote biometrics in public spaces. ^{22,23}
Export controls	Licences for selling surveillance technology abroad, with human rights impact assessments before transfers. ²⁴
Vendor and customer checks	“Know Your Vendor” and “Know Your Customer” checks on who builds and buys the tools. ²⁵

¹⁵ Biometric Update. UN rights report calls for moratorium on remote biometrics in public (September 2021).

<https://www.biometricupdate.com/202109/un-rights-report-calls-for-moratorium-on-remote-biometrics-in-public>

¹⁶ OHCHR. A/HRC/60/45: The right to privacy in the digital age (report of the High Commissioner... (See earlier note or bibliography.)

¹⁷ United Nations. Universal Declaration of Human Rights (adopted 10 December 1948)... (See earlier note or bibliography.)

¹⁸ OHCHR. International Covenant on Civil and Political Rights, Article 17. <https://www.ohchr.org/sites/default/files/ccpr.pdf>

¹⁹ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

²⁰ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

²¹ UK Government. The Pall Mall Process Code of Practice for States (April 2025).

<https://assets.publishing.service.gov.uk/media/67f8f85b04146682e61bc867/The-Pall-Mall-Process-Code-of-Practice-for-States.pdf>

²² OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

²³ Biometric Update. UN rights report calls for moratorium on remote biometrics in public... (See earlier note or bibliography.)

²⁴ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

²⁵ UK Government. The Pall Mall Process Code of Practice for States (April 2025)... (See earlier note or bibliography.)

3. Key Definitions

These definitions are adapted from the UN and other sources listed in the bibliography. Learn them, because you will use them in speeches and clauses.

Term	Meaning
Privacy	The right not to be subjected to arbitrary interference with one's private life, family, home or correspondence. ²⁶
Surveillance	Monitoring people's communications, movements, online activity or identity.
Targeted surveillance	Watching specific people, usually with a legal reason and approval.
Mass surveillance	Collecting data on large numbers of people without suspicion of each one.
Biometric data	Data about the body used to identify a person, such as a face, fingerprints or irises. ²⁷
Remote biometric recognition	Identifying people from a distance, most often by facial recognition, in real time or from recordings. ²⁸
Digital ID	An electronic identity system that often stores biometric data, such as Afghanistan's e-Tazkira. ²⁹
Spyware	Software that secretly takes control of a device to read messages, collect data and track the user. ³⁰
Commercial spyware	Spyware built and sold by private companies, usually to governments. The Pall Mall Process calls the wider class "commercial cyber intrusion capabilities". ³¹
Zero-click attack	An attack that infects a device without the owner clicking anything.
Encryption	Scrambling messages so that only the sender and receiver can read them. It protects privacy and rights. ³²
Backdoor	A deliberate weakness in security that lets others bypass encryption. The UN urges states not to require them. ³³
Client-side scanning	Systematic screening of material on a user's own device. ³⁴

²⁶ United Nations. Universal Declaration of Human Rights (adopted 10 December 1948)... (See earlier note or bibliography.)

²⁷ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022).

<https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans>

²⁸ Biometric Update. UN rights report calls for moratorium on remote biometrics in public... (See earlier note or bibliography.)

²⁹ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022)... (See earlier note or bibliography.)

³⁰ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

³¹ Freedom House. How the Pall Mall Process Can Help Combat Commercial Spyware Abuse. <https://freedomhouse.org/article/how-pall-mall-process-can-help-combat-commercial-spyware-abuse>

³² OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

³³ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

³⁴ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

Term	Meaning
Arbitrary	Without a lawful, reasonable and justified basis. ³⁵
Necessity and proportionality	Tests that the measure is really needed and no greater than the harm it prevents. ³⁶
Chilling effect	When people stop speaking, organising or reporting because they fear being watched.
Transnational repression	Authoritarian governments targeting dissidents, journalists and activists outside their own borders. ³⁷
Export controls	Government rules and licences that limit the sale of sensitive technology abroad. ³⁸
Human rights impact assessment	A study of the risks to rights before a technology is sold or deployed. ^{39,40}
Moratorium	A temporary pause on a practice until safeguards are in place. ⁴¹
Data protection law	Rules about how personal data may be collected, stored and shared, and who enforces them. ⁴²
Non-binding	A text, such as a UN resolution or the Pall Mall Code, that states agree to follow politically but that is not enforceable law. ^{43,44}
Accountability	Making sure that people and institutions answer for what they do, through oversight, reporting and remedies.

³⁵ United Nations. Universal Declaration of Human Rights (adopted 10 December 1948)... (See earlier note or bibliography.)

³⁶ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

³⁷ US Department of Commerce. Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities (3 November 2021). <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>

³⁸ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

³⁹ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

⁴⁰ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022)... (See earlier note or bibliography.)

⁴¹ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

⁴² CIPESA. Insights into Zambia's Data Protection Act 2021. <https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf>

⁴³ UK Government. The Pall Mall Process Code of Practice for States (April 2025)... (See earlier note or bibliography.)

⁴⁴ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

4. Case Studies

These cases show the problems and some responses in real life. Facts come from the sources in the bibliography. Numbers are estimates and may change, so check dates and methods. **You must represent your assigned country's view.**

4.1 The Pegasus Project (2021)

In July 2021 a consortium of 17 media organisations, working with Forbidden Stories and Amnesty International, reported on a leaked list of more than 50,000 phone numbers linked to clients of Israel's NSO Group. The numbers included more than 180 journalists, as well as ministers, presidents, prime ministers and activists. At least 11 governments were suspected of being NSO customers, including Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India and Togo. NSO said Pegasus is "only intended for use against criminals and terrorists" and denied the allegations.⁴⁵

4.2 Blacklists and lawsuits (2021 and 2025)

On 3 November 2021 the US Commerce Department added NSO Group and Candiru (Israel) to its Entity List, restricting exports to them. It said they supplied spyware to governments that used it to target officials, journalists, activists, academics and embassy workers.⁴⁶ In May 2025 a US jury found NSO liable for hacking about 1,400 WhatsApp users, and awarded about \$168 million, of which about \$167.3 million was punitive. NSO said it would appeal.⁴⁷ A judge later reduced the penalty, so check the figure.⁴⁸

4.3 Afghanistan: biometric data left behind (2021–2022)

Before 2021, several systems held sensitive biometric data on Afghans, including the e-Tazkira national ID, a US military database covering about 2.5 million people, and payroll systems for police, soldiers and judges. Human Rights Watch found that the Taliban gained handheld biometric devices and used fingerprints and iris scans to identify former security personnel and judges, though access to some systems is disputed.⁴⁹ HRW documented 47 killings or disappearances of former security personnel between 15 August and 31 October 2021, and urged risk assessments **before** deployment and plans for data destruction in conflict zones.⁵⁰

4.4 Zambia's 2025 cyber laws and data protection

In April 2025 Zambia's Parliament passed the Cyber Security Act and the Cyber Crimes Act.⁵¹ The Cyber Security Act requires communications providers to install systems that can facilitate real-time interception of communications (section 39) and sets up a Central Monitoring and Coordination Centre (section 21).⁵²

⁴⁵ Business and Human Rights Resource Centre. Investigation finds NSO Group spyware sold to... (See earlier note or bibliography.)

⁴⁶ US Department of Commerce. Commerce adds NSO Group and other foreign companies to Entity List... (See earlier note or bibliography.)

⁴⁷ CyberScoop. NSO Group owes \$168M in damages to WhatsApp over spyware infections, jury says (May 2025). <https://cyberscoop.com/nso-group-owes-whatsapp-over-spyware-infections-jury/>

⁴⁸ Cybernews. Judge shrinks NSO penalty in WhatsApp hack case. <https://cybernews.com/news/nso-group-whatsapp-fine-reduced/>

⁴⁹ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022)... (See earlier note or bibliography.)

⁵⁰ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022)... (See earlier note or bibliography.)

⁵¹ CIPESA. Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights (May 2025). <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/>

⁵² CIPESA. Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights (May 2025)... (See earlier note or bibliography.)

Groups including CIPESA and Bloggers of Zambia criticised vague wording, weak judicial oversight, interception orders made without hearing the affected person, and offences that could chill criticism.⁵³ Consider the government's aim of fighting cybercrime too. Zambia's 2021 Data Protection Act protects sensitive data, but critics say its national security exemption is broad.⁵⁴

4.5 The EU's limits on biometric surveillance

The EU AI Act bans real-time remote biometric identification in publicly accessible spaces for law enforcement, with three narrow exceptions: searching for specific victims of kidnapping, trafficking or sexual exploitation; preventing a specific, imminent terrorist threat; and identifying suspects of serious crimes. Each use needs prior judicial or independent authorisation. It also bans systems that use biometrics to infer race, political opinions, religion or sexual orientation. These bans have applied since 2 February 2025.⁵⁵

4.6 The Pall Mall Process on commercial spyware

The UK and France began the Pall Mall Process in 2024 to address the "proliferation and irresponsible use" of commercial cyber intrusion capabilities. In April 2025, 25 governments, including the United States, signed a Code of Practice for States, which is voluntary and non-binding.⁵⁶ It rests on four pillars: accountability, precision, oversight and transparency, and urges export licensing that weighs the risk of internal repression and serious human rights abuses.⁵⁷ Critics say its human rights language is qualified, and that it ignores transnational repression.⁵⁸ Civil society groups have also published recommendations on industry guidelines for these tools.⁵⁹

⁵³ CIPESA. Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights (May 2025)... (See earlier note or bibliography.)

⁵⁴ CIPESA. Insights into Zambia's Data Protection Act 2021... (See earlier note or bibliography.)

⁵⁵ regulation-ai.eu. EU AI Act Prohibited Practices (Art. 5): in force since February 2025. <https://www.regulation-ai.eu/en/prohibited-practices/>

⁵⁶ Freedom House. How the Pall Mall Process Can Help Combat Commercial Spyware Abuse... (See earlier note or bibliography.)

⁵⁷ UK Government. The Pall Mall Process Code of Practice for States (April 2025)... (See earlier note or bibliography.)

⁵⁸ Freedom House. How the Pall Mall Process Can Help Combat Commercial Spyware Abuse... (See earlier note or bibliography.)

⁵⁹ Amnesty International Security Lab. Essential elements for ensuring the Industry Guidelines for Commercial Cyber Intrusion Capabilities deliver on their potential: joint civil society submission (September 2026). <https://securitylab.amnesty.org/latest/2026/09/essential-elements-for-ensuring-the-industry-guidelines-for-commercial-cyber-intrusion-capabilities-deliver-on-their-potential-joint-civil-society-submission/>

5. Major Actors

5.1 Countries and regions

Your delegation may represent any country, and your country may not be listed here. The table shows broad patterns only. **Always check your country's recent statements, laws and policies before you rely on them.**

Type of country	What to expect
Home states of spyware makers	Balance security and industry interests with export controls, and may stress that the tools fight crime. NSO Group and Candiru are Israeli companies. ⁶⁰
States named as spyware customers	Several states named in the Pegasus Project reporting have disputed or not confirmed it. Expect them to stress national security and sovereignty. ⁶¹
Regulating democracies and blocs	Push for binding limits, such as the EU's biometric rules and US export restrictions. ^{62,63}
Developing states building digital systems	Want digital ID, cyber laws and security tools, while facing criticism over oversight, as in Zambia. ^{64,65}
Conflict and post-conflict states	Stress the danger of data falling into the wrong hands, as in Afghanistan. ⁶⁶

Disagreements tend to come over **national security, binding versus voluntary rules** and **who pays for oversight**.

5.2 Organisations and networks

- **The Human Rights Council, OHCHR and the Special Rapporteur on privacy.** They set standards, report on abuses and recommend action.^{67,68,69}
- **Civil society and media.** Amnesty International, Forbidden Stories, Human Rights Watch, CIPESA and Freedom House investigate, document and campaign.^{70,71,72,73}

⁶⁰ US Department of Commerce. Commerce adds NSO Group and other foreign companies to Entity List... (See earlier note or bibliography.)

⁶¹ Business and Human Rights Resource Centre. Investigation finds NSO Group spyware sold to... (See earlier note or bibliography.)

⁶² regulation-ai.eu. EU AI Act Prohibited Practices (Art. 5): in force since February 2025... (See earlier note or bibliography.)

⁶³ US Department of Commerce. Commerce adds NSO Group and other foreign companies to Entity List... (See earlier note or bibliography.)

⁶⁴ CIPESA. Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights (May 2025)... (See earlier note or bibliography.)

⁶⁵ CIPESA. Insights into Zambia's Data Protection Act 2021... (See earlier note or bibliography.)

⁶⁶ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022)... (See earlier note or bibliography.)

⁶⁷ UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council... (See earlier note or bibliography.)

⁶⁸ OHCHR. Human Rights Council creates mandate of Special Rapporteur on the right to privacy (26... (See earlier note or bibliography.)

⁶⁹ OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns... (See earlier note or bibliography.)

⁷⁰ Business and Human Rights Resource Centre. Investigation finds NSO Group spyware sold to... (See earlier note or bibliography.)

⁷¹ Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022)... (See earlier note or bibliography.)

⁷² CIPESA. Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights (May 2025)... (See earlier note or bibliography.)

⁷³ Freedom House. How the Pall Mall Process Can Help Combat Commercial Spyware Abuse... (See earlier note or bibliography.)

6. Preparing for Committee

6.1 Questions a strong resolution answers

1. **What problem does it solve?** State surveillance, biometric data, or commercial spyware? In which place and for whom?
2. **Who acts?** Name who will do it: states, courts, companies, the OHCHR or the Special Rapporteur.
3. **Does it pass the test?** Is it lawful, necessary and proportionate, with real oversight?
4. **Does it protect remedies?** Can people discover, challenge and seek redress?
5. **Is it realistic?** Would states with very different resources be able to carry it out?
6. **Does it recognise security needs?** Fighting serious crime and terrorism is a legitimate aim.
7. **How will it be checked?** Add reporting, a review date and a role for the Special Rapporteur.
8. **Can it win support?** Will states from different regions and views vote for it?

6.2 Guiding questions for your research

1. What laws does your country have on surveillance, interception and data protection?
2. Does your country make, buy or export surveillance technology or spyware?
3. Does your country use biometric ID, facial recognition or large databases?
4. Has your country been named in reports of spyware or surveillance abuse?
5. What has your country said or voted at the Human Rights Council on privacy?
6. Has your country signed the Pali Mall Code, or the ICCPR?
7. Which countries share your goals, and where would you compromise?

6.3 Where to research

- **OHCHR** reports on the right to privacy in the digital age, and Special Rapporteur reports.
- **Amnesty International Security Lab, Citizen Lab and Human Rights Watch**, for investigations.
- **CIPESA and Freedom House**, for African and global digital rights.
- **Your country's laws and statements** at the Human Rights Council and the UN.

Bibliography

Amnesty International Security Lab. Essential elements for ensuring the Industry Guidelines for Commercial Cyber Intrusion Capabilities deliver on their potential: joint civil society submission (September 2026).

<https://securitylab.amnesty.org/latest/2026/09/essential-elements-for-ensuring-the-industry-guidelines-for-commercial-cyber-intrusion-capabilities-deliver-on-their-potential-joint-civil-society-submission/>

Biometric Update. UN rights report calls for moratorium on remote biometrics in public (September 2021).

<https://www.biometricupdate.com/202109/un-rights-report-calls-for-moratorium-on-remote-biometrics-in-public>

Business and Human Rights Resource Centre. Investigation finds NSO Group spyware sold to governments used against activists, politicians and journalists; company denies allegations (Pegasus Project, July 2021). <https://www.business-humanrights.org/en/latest-news/nso-group-spyware-sold-to-governments-used-to-target-activists-politicians-journalists-according-to-pegasus-project-investigation-company-denies-allegations/>

- CIPESA. Insights into Zambia's Data Protection Act 2021. <https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf>
- CIPESA. Zambia's Cybersecurity and Cybercrimes Laws Raise Alarms for Digital Rights (May 2025). <https://cipesa.org/2025/05/zambias-cybersecurity-and-cybercrimes-laws-raise-alarms-for-digital-rights/>
- Cybernews. Judge shrinks NSO penalty in WhatsApp hack case. <https://cybernews.com/news/nso-group-whatsapp-fine-reduced/>
- CyberScoop. NSO Group owes \$168M in damages to WhatsApp over spyware infections, jury says (May 2025). <https://cyberscoop.com/nso-group-owes-whatsapp-over-spyware-infections-jury/>
- Freedom House. How the Pall Mall Process Can Help Combat Commercial Spyware Abuse. <https://freedomhouse.org/article/how-pall-mall-process-can-help-combat-commercial-spyware-abuse>
- Human Rights Watch. New Evidence that Biometric Data Systems Imperil Afghans (30 March 2022). <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans>
- OHCHR. A/HRC/60/45: The right to privacy in the digital age (report of the High Commissioner, 29 August 2025). <https://www.ohchr.org/en/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high>
- OHCHR. Human Rights Council creates mandate of Special Rapporteur on the right to privacy (26 March 2015). <https://www.ohchr.org/en/press-releases/2015/03/human-rights-council-creates-mandate-special-rapporteur-right-privacy>
- OHCHR. International Covenant on Civil and Political Rights, Article 17. <https://www.ohchr.org/sites/default/files/ccpr.pdf>
- OHCHR. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns (press release, 16 September 2022). <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>
- regulation-ai.eu. EU AI Act Prohibited Practices (Art. 5): in force since February 2025. <https://www.regulation-ai.eu/en/prohibited-practices/>
- UK Government. The Pall Mall Process Code of Practice for States (April 2025). <https://assets.publishing.service.gov.uk/media/67f8f85b04146682e61bc867/The-Pall-Mall-Process-Code-of-Practice-for-States.pdf>
- UN Office of the High Commissioner for Human Rights. Welcome to the Human Rights Council. <https://www.ohchr.org/en/hr-bodies/hrc/about-council>
- United Nations. Universal Declaration of Human Rights (adopted 10 December 1948). <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
- US Department of Commerce. Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities (3 November 2021). <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>

Guide done by:

Malenji Arthur Jonah

Secretary General, LOTSMUN 2026