Spyware Accountability Mechanisms Framework

A Guide to Support Discussions Around Spyware Accountability

Freedman Consulting, LLC

September 2023

Table of Contents

Introduction and Overview

Commercial spyware poses a significant challenge to free societies worldwide, as it threatens human rights defenders, marginalized communities, and advocates of free speech globally. Efforts to rein in the global market in commercial spyware, limit these tools' development, prevent their deployment, and otherwise mitigate harms have made significant progress in recent years, but many problems remain stubbornly unsolved.

On behalf of the Ford Foundation and Open Society Foundations, Freedman Consulting, LLC developed this report to create a framework for discussing a wide range of levers for advancing commercial spyware accountability. It is based on perspectives from researchers, advocates, commercial actors, funders, and others. This proposed spyware accountability mechanisms framework report is intended to provide a shared basis for discussion and planning among relevant actors in the spyware accountability space, particularly in the American and European contexts. While some international examples are highlighted throughout this report, continued research is needed to assess effective spyware accountability levers for broader global applications.

This document should be understood as a thorough, but brief and non-exhaustive, high-level proposed framework of mechanisms that can serve as a shared basis for discussion and planning among relevant actors in the spyware accountability space. This document is meant to spark discussion on various levers of spyware accountability and create a shared language for further development. As such, it does not seek to weigh relative merits of levers or strategies, nor does it assess challenges and opportunities to advancing spyware accountability more broadly. Addressing these questions is the vital work of future study, discussion, and refinement.

Defining the Goal: Eliminating or Mitigating Spyware Harms

The significant and growing challenge of commercial spyware threatens human rights defenders, democracy and free speech advocates, and marginalized communities around the world. Spyware tools enable repression and abuse, and their increasingly widespread deployment threatens visions of free, just, and open societies. From Mexico and Saudi Arabia to Sudan and Thailand, communities across the world have been impacted by the booming spyware industry. In 2021, the Pegasus Project revealed the widespread reach of NSO Group's Pegasus spyware, which was employed by over 50 countries to surveil at least 180 journalists across the world, in addition to human rights defenders, academics, political leaders, and others.

The rapid growth of the spyware industry and its global marketplace has affected numerous levels of society. The industry has had privacy impacts on everyday consumers, resulted in security threats for activists or journalists exposing injustices in their home countries, and contributed to the intra- or cross-state surveillance of civilians.

Addressing these harms, however, has proven difficult. Establishing a widely shared definition of spyware tools can be a challenging exercise. Companies that develop these pernicious tools operate largely in the shadows, with an (at-best) fragmented oversight and regulatory system. The deployers of spyware tools are often state actors, and public interest researchers face a cat-and-mouse game of attempting to detect and respond to infections as spyware purveyors race to develop better tools. This document is intended to support a conversation on how to push back and advance the cause of spyware accountability.

Commercial spyware is one key component of a larger body of work on surveillance reform and data privacy. Spyware tools are often used alongside other rights abuses – for example, in India, activists were targeted with Pegasus in addition to having false evidence planted on their devices through other hacking tools. Although these larger concerns are outside the scope of this report, spyware and the methods for spyware accountability are an important and useful area of focus within the larger landscape.

Experts working on these issues have made it clear that these spyware accountability levers can achieve a myriad of objectives. Specific mechanisms for change (accountability levers) fall along a broad spectrum of approaches, including national action, international agreements, investor engagement, corporate action, strategic litigation, technical interventions, or the use of media and education campaigns. This document attempts to catalogue different approaches to enable an effective discussion, and it lays out mechanisms of change largely along the lines of what entity or group of people would take action to implement them.

Defining the Goal: Live Questions and Potential Tensions

Spyware accountability is a domain with many live questions about the core objectives, best strategies, and most effective methods for mitigating spyware harms. Resolving these questions will likely require confronting a wide variety of potential tensions. While weighing the merits of particular objectives, strategies, or mechanisms is beyond the scope of this report, several factors nonetheless emerged during the research process and are highlighted here to support further discussion among stakeholders.

Experts consulted for this document – and those working on spyware issues more broadly – were often divided on precise objectives for accountability work, even with a universal agreement that fighting commercial spyware is vital. Most stated that an outright ban on the use of these tools should be the objective, though many also expressed that bringing these tools into a better regulatory framework would be tremendously beneficial, even if advocates never win a full ban. (One argued for divorcing efforts to fight spyware from broader surveillance reform efforts altogether.) Several experts also emphasized the benefits of an accountability approach that puts significant emphasis on reducing harm. Many experts expressed concerns about the political will and technical challenges to implementing bans or regulations on spyware, but they and others also indicated their hope for progress as spyware harms have made their way into public awareness. Some also highlighted the need for persistence, arguing that this industry has become so entrenched that efforts to uproot it will require commitment and long-term focus.

The mechanisms for change listed in this document attempt to cover a wide range of approaches to mitigating spyware harms, include both long- and short-term efforts, domestic and international actions, technical and normative levers, and preventative and reactive strategies. Efforts to prioritize these accountability mechanisms are beyond the scope of this report, but key factors might include:

- Probability of success
- Level of impact if successful
- Resources needed to implement the action
- Methods and likelihood of enforcement
- Desired focus on specific harms inflicted on civil society (e.g., broad state surveillance versus individual surveillance of activists or journalists)
- Ideal timelines for action
- Geographic targets / actors implicated (e.g., private entity versus states)
- Aligned partners who can help advance accountability actions
- Desired outcomes of any action taken against bad actors

Research Objectives & Methodology

This report seeks to provide a menu of levers and establish a taxonomy for discussing levers to advance spyware accountability. Recommended actions for spyware accountability exist at various levels; some are speculative, while other proposed levers are derived from real-world examples. These levers may also overlap or operate across recommended types. This report is intended to be thorough, but non-exhaustive. Ultimately, there may be many more approaches to advancing spyware accountability than are captured here, and this report generally does not explore large-scale reforms beyond the spyware policy space (such as larger data economy regulations).

To develop this report, Freedman Consulting interviewed 13 spyware accountability experts, field leaders, and stakeholders to surface insights about high-level approaches to mitigating harms from spyware and related tools, like stalkerware. Interviewees included human rights lawyers and journalists, advocates and experts at civil society organizations, technical professionals, and academic experts. While the definition of spyware is often contested, this report does not focus on definition variances or alignment.

To supplement interview findings, Freedman Consulting also conducted a substantial research scan focusing primarily on the United States and Europe on both policy and non-policy levers from media sources and relevant stakeholders. The research scan was constrained to sources dating back to 2018, with a focus on levers of accountability. Initial research began with scans of major news media and technology-specific news sources as well as the online publications of relevant stakeholders. Iterative research was conducted throughout the research process to investigate new areas of inquiry. Additional information about the research methodology is provided in the appendix.

A Note on Specific Geographies

It is essential to acknowledge that much of this report contains ideas for spyware accountability mechanisms sourced from experts based in the Global North that often propose action in those same geographies. Some of this focus is driven by a disparity in resources for civil society, as well as global power differentials. However, there is a hope that many approaches highlighted here could also be implemented in or recontextualized for other geographies.

Commercial spyware is a global menace that threatens human rights and inclusive democracy, and solutions must be similarly global. While funding from Global North investors may support the growth of spyware companies, it also causes harm in other regions. Throughout the development of this report, experts highlighted potential synergies in needs and opportunities across regions, including:

- Increasing collaboration among international and local organizations documenting spyware harms to achieve greater awareness and impact.
- Creating and strengthening international norms on responsible disclosures.
- Establishing universal jurisdiction to develop global accountability systems.
- Providing resources to investigate spyware activities at a regional level, so that findings and actions are rooted in specific contexts.
- Leveraging geography-agnostic, broadly applicable levers, such as corporate accountability and transparency actions.
- Providing support and protection for activists working on spyware accountability across the world.
- Standardizing the documentation of spyware cases.

Moving forward, there are opportunities to continue exploring and uplifting actions and recommendations from other regions, particularly from voices and organizers in Latin America, Africa, and Asia.

I. Mechanisms of Change: National Action

Overview

National governments have a crucial role to play in preventing or limiting the development and use of spyware, as well as promoting accountability after deployment. Countries are often the customers of spyware companies, house the companies that produce spyware technology, or are victims of commercial spyware use.

National governments can ban the production, sale, possession, or use of spyware by public and private entities, regulate and establish reporting and disclosure requirements for spyware companies, take measures to protect government employees and agencies, and restrict funding of spyware companies. Countries also can regulate and influence entities in their jurisdictions, like local governments, companies, and individuals. National governments can take steps to deter individuals from working for spyware companies through revolving door policies. Finally, national governments can mandate that states or municipalities in their purview establish spyware bans or regulations and influence the actions of individuals or private entities. Key challenges to national action, however, include the domestic and international political circumstances that shape the political possibilities and will to act.

Additionally, national intelligence and police agencies are some of the most significant producers and users of surveillance technology generally, of which the commercial spyware focused on in this report is just one part. Although general limits and reform to the surveillance state could also serve to limit spyware harms, state-developed surveillance and the harms associated lie outside the scope of this report.

National action includes five main categories of levers:

A. Bans
B. Regulations
C. Reporting and Transparency: Disclosure Requirements
D. Reporting and Transparency: Threats & Harms
E. Litigation-Related Action
F. Other Policies

A. Bans

1. **Ban the production, sale, possession, and use of spyware by all governmental, public, and private entities.** A full ban on spyware could cover all types of actors at all stages of production and use, with mechanisms for enforcement and consequences for violations. If such a ban is enacted, protecting research access to spyware products may be important, potentially through a carveout for the possession of spyware technology for research and academic purposes.
    - *Example*: Greece's parliament passed a bill making the private use of spyware a felony and criminalizing the sale or possession of spyware in 2022. The bill also

created a counterintelligence academy for the country's intelligence service staff and established a unit to investigate breach of duty cases. However, enforcement may be lacking.

2. **Ban key actors from entering countries and freeze the assets of foreign actors from states perpetuating spyware harms.** Many countries have sanctions laws that could potentially be used to deter spyware development by imposing consequences on individuals or firms associated with spyware production, export, and use.
    - *Example:* In the United States, the Global Magnitsky Act allows the executive branch to impose sanctions against anyone in the world for human rights or significant corruption violations, freezing any assets that they have in U.S. banks and banning them from the U.S. financial system. Similar provisions in other countries could enable countries to impose consequences for individuals propagating spyware harms.
3. **Limit or refuse to grant export licenses to spyware companies.** Countries where spyware is developed can set higher standards for other nations to purchase and use spyware tools or reject such requests altogether. These reforms could intersect with efforts to improve global export controls.
    - *Example*: The Israeli government reportedly blocked licenses for the NSO Group to sell Pegasus to Ukraine and Estonia in March 2022 due to concerns that selling the cyberweapon to the two countries would hurt Israel's relationship with the Russian government.
4. **Sanction investors in spyware companies**. Countries can deter private equity, venture capital, and other firms from funding spyware companies by including leaders at these firms in sanctions that are enacted in response to spyware harms. Casting a wider net when imposing sanctions could increase the power of existing and planned sanctions processes.
5. **Expand national bans on commercial spyware possession, sale, and use to state and local governments.** Countries with existing bans or limitations on the national government's use of commercial spyware could extend those restrictions to local governments and private entities.
    - *Example:* American President Biden's recent executive order prohibiting "operational use by the United States Government of commercial spyware that poses risks to national security or has been misused by foreign actors to enable human rights abuses around the world" could be expanded to include state and local governments.

B. Regulations

1. **Establish limits on how national intelligence agencies use commercial spyware.** Creating and strengthening regulations on the use of commercial spyware by intelligence agencies and other parts of the national government could forward surveillance reform efforts generally.

- *Example*: In the United States, the 2023 National Defense Authorization Act (NDAA) gives the Director of National Intelligence (DNI) the authority to mandate how intelligence agencies use spyware, including the authority to prohibit intelligence agencies from procuring or licensing commercial spyware.

2. **Establish a uniform national regulatory system for spyware.** Countries can establish an independent oversight mechanism for companies selling spyware, monitor and investigate their use, and ensure that use is consistent with international human rights law and other regulations.
3. **Use export controls and sanctions to limit the ability of citizens to enter and participate in the spyware industry.** Countries can establish export control rules to prohibit or restrict their citizens from supporting the development of products counter to the national interest, such as spyware and other surveillance technologies.
    - *Example:* In October 2022, the American Bureau of Industry and Security (BIS) expanded export controls on the semiconductor industry and restricted the involvement of American citizens in Chinese semiconductor chip companies. The Export Administration Regulation (EAR) essentially places sanctions on services in the industry. This model could be adapted for the commercial spyware industry.
4. **Strengthen procurement standards for firms that provide goods or services to the national government related to surveillance.** Procurement standards could ensure that firms providing products to the government are not also involved in spyware production or financing the spyware industry. Standards could also increase the digital security requirements for products sold to governments. These rules could be established through executive orders requiring software vendors selling to the national government to meet certain cybersecurity standards.
5. **Enact large-scale government surveillance reform.** The use of spyware tools by governments is often a function of a larger surveillance state. Efforts to restrain intelligence and law enforcement agencies from surveilling their citizens as well as foreign nationals could reduce the size of the market for these tools, potentially limiting the development and use of commercial spyware.

C. Reporting and Transparency: Disclosure Requirements

1. **Require domestic spyware firms to disclose clients and other information.** Regular mandatory reporting of clients would increase transparency and deter potential clients of spyware firms. Domestic spyware companies could also be required to make regular public disclosures about the export of their products to other countries.
2. **Mandate reporting by national surveillance and national security agencies with a comprehensive inventory of the "revolving door" between the government and the cybersurveillance industry.** Many countries have laws regulating employment turnover between the public and private sector, particularly in high-level positions. These regulations could also include reporting requirements to help better understand the relationship between state-trained expertise and the spyware industry.

- *Example:* In the United States, the White House or Congress could require U.S. agencies to report when employees with advanced technical expertise leave government roles to work for private-sector surveillance firms or foreign entities.

3. **National finance regulators can use their regulatory powers to require reporting for spyware companies.** Government agencies that regulate financial transactions can require spyware companies to establish due diligence on the use of their products and mandate public reporting of financial records on the sale, export, and use of their products.
    - *Example:* In the United States, the Securities and Exchange Commission (SEC) rules could mandate reporting and strong due diligence for spyware and other surveillance companies that provide products to the federal government. The SEC has the power to "register, regulate, and oversee brokerage firms, transfer agents, and clearing agencies as well as the nation's securities self-regulatory organizations." The SEC also has disciplinary powers over regulated entities and can require reporting from companies with publicly traded securities. With these powers, the SEC could require spyware-related companies and companies with dual-use products to conduct robust due diligence on the usage of their products and require public reporting for the sale, export, and clientele of their products.

D. Reporting and Transparency: Threats & Harms

1. **Add spyware and other digital practices to existing human rights assessments and reporting by national bodies.** Countries with existing reporting requirements for human rights domestically or internationally could add spyware vulnerabilities and harms assessments as specific areas of research to their reporting processes.
    - *Example:* The European Union High Representative for Foreign Affairs and Security Policy's 2021 global report highlighted harms from spyware and threats to human rights.
    - *Example:* In the United States, the State Department could add spyware assessments to their annual Country Reports on Human Rights Practices. Human rights reports require annual assessments of human rights conditions in countries around the world. By integrating reporting on digital practices and spyware, the State Department could better evaluate human rights conditions worldwide.
2. **Require reporting from national intelligence agencies to elected officials assessing the threat posed by spyware.** Stronger reporting on spyware vulnerabilities and harms in countries around the world can help governments better address weaknesses and assess next steps.
    - *Example*: In the United States, the 2023 NDAA created reporting requirements on the threat spyware poses to U.S. national security. To expand this effort, Congress or the White House could require the DNI to create and submit a watch list of foreign spyware firms that present a risk to intelligence agencies to

Congress. (Previous legislation required a similar report from the State Department.)

3. **Publish reports on the use of foreign commercial spyware against diplomats and the national government's response to cyberattacks on government officials.** Public transparency on vulnerabilities faced by public officials and the national government could promote learning in the space for the detection, investigation, and reporting of spyware attacks worldwide. Public transparency can also promote deterrence for spyware companies and states utilizing spyware technology.
4. **Establish civilian control boards over surveillance and spyware use by government actors.** Civilian oversight boards can provide external review for governmental use of surveillance and spyware and promote transparency and additional regulation.
5. **Improve vulnerability disclosure policies to better address the global zero-day exploits market.** Government agencies could more efficiently and consistently disclose discovered vulnerabilities to technology companies to allow for more effective patching of security vulnerabilities. Many states lack effective vulnerability disclosure processes (or explicit processes altogether), exacerbating a lack of government transparency and leaving individuals vulnerable to spyware attacks. Countries that do have these policies may not sufficiently weigh the public interest in disclosing more vulnerabilities faster so that they can be patched.
    - *Example:* The United States vulnerability equities process (VEP) evaluates whether to withhold or disclose software security vulnerabilities to the public. Although the VEP provides a framework for evaluating disclosure, it lacks transparency in timeline, coverage, and use, as government entities do not disclose what vulnerabilities do not go through the process or how long the process takes. Other countries, like Australia and the United Kingdom, have similar processes.

E. Litigation-Related Action

1. **Enact legislation that gives victims clearer rights to sue spyware vendors for spyware harm.** Strategic litigation strategies are hindered by strict jurisdictional restrictions and other requirements when suing for spyware-related harms. Governments can make it easier for spyware-related litigation to reach evidence-gathering stages, creating more opportunities for the investigation of spyware harms.
2. **Enact national legislation confirming that individuals have a private right of action against foreign states in cases related to spyware.** Questions of state or sovereign immunity are often used by spyware companies to attempt to skirt accountability in litigation efforts. NSO Group, an Israeli spyware maker, filed for immunity in a lawsuit by WhatsApp in the United States; the Kingdom of Bahrain attempted to claim state immunity in a lawsuit in London in 2023; and the Kingdom of Saudi Arabia tried but ultimately failed to claim immunity in a spyware-related case in the UK in 2022. By explicitly allowing foreign spyware companies to be sued, national governments can remove a key challenge to litigation strategies.

3. **Implement universal jurisdiction provisions.** National governments can also address jurisdiction-related issues in spyware litigation by enacting universal jurisdiction provisions for spyware harms. Such an approach could improve access to justice by allowing litigation and prosecution against perpetrators of spyware harms, regardless of their or their victims' nationalities.

F. Other Policies

1. **Conduct an independent, impartial, and transparent investigation into all alleged cases of targeted surveillance abuse.** Countries could establish a national body to conduct investigations into surveillance and spyware abuse. This national body can also investigate spyware harms and produce recommendations for domestic spyware mitigation strategies.
    - *Example*: The PEGA Committee, a European Union parliamentary panel, investigates abuses of spyware technology and produces reports and recommendations in relation to the use of Pegasus and other surveillance spyware.
    - *Example:* In 2021, India's supreme court mandated the creation of an independent committee to investigate the Indian government 's use of Pegasus. The committee found malware in various devices submitted to it for investigation, but did not find conclusive proof of the use of Pegasus specifically. The committee was hindered by a lack of cooperation from the government.
2. **Condition foreign aid formally or informally to restrict the use of spyware.** Countries could require other nations receiving foreign aid to comply with certain rules and regulations around the production, export, and use of spyware. Absent formal conditions, foreign aid programs may also provide an opportunity to rein in spyware abuses through informal diplomatic or public pressure and other means.
3. **Extend and enforce revolving door restrictions for people with specialized expertise.** Revolving door restrictions can limit people who leave government intelligence agencies from working for foreign countries, for private contractors doing foreign business, or for tech companies for a certain amount of time.
    - *Example*: The American 2023 NDAA authorized the president to "prohibit Americans from providing support to that surveillance agency or any of the dozens of security agencies around the world that have used advanced technology — such as the NSO Group's Pegasus spyware — against journalists, human rights defenders, and opposition politicians." These authorities add to an existing ability to restrict employment with foreign militaries.
4. **Establish clear national digital security policies to protect government data and employees.** Governments can deter spyware attacks by strengthening their defensive capacities through robust data security practices. Stronger digital security practices could prevent spyware attacks on national government entities and mitigate harm in the event of a spyware attack.

5. **Integrate spyware accountability into existing anti-corruption and government accountability efforts.** National governments with existing anti-corruption and government accountability efforts and working groups could integrate spyware accountability efforts into their mandates. This kind of approach may be particularly important for geographies where spyware abuses are closely linked with corruption.
6. **Use criminal authority to deter the use of spyware.** National governments can charge and prosecute foreign individuals and countries involved with spyware abuses. Countries that discover foreign nationals or foreign governments committing spyware abuses in their territory or against their citizens could charge them with conspiracy to commit an offense against the government.
    - *Example:* The U.S. Justice Department charged six Russian military intelligence officers with "conspiracy to commit an offense against the United States" for their involvement in a global hacking movement. The indictment was unsealed in October 2020.

II. Mechanisms of Change: International Agreements & Action

Overview

International agreements and action include all actions involving more than one national government, including international entities like the European Union, United Nations, and African Union. International bodies can establish binding and non-binding agreements to rein in spyware, as well as coordinate cross-border efforts to enact sanctions, export controls, and oversight efforts. Both bans and regulations can target spyware at multiple stages in its lifecycle, including development, export, use, and accountability. Regulations, export controls, and sanctions at their strongest can potentially function as de facto bans and strategies for deterrence could have a robust impact on spyware producers, states of proliferation, and states using spyware technology.

A key challenge to these levers, like for national action levers, is the need for widespread political will and favorable global political conditions for passage and adherence. Enforcement is another challenge. However, global norms and rules against the product, spread, and use of spyware could significantly forward spyware accountability and contribute to the efficacy of other levers outlined.

International agreements and action falls into three broad categories:

A. Bans and Moratoria
B. Sanctions, Oversight, and Export Controls
C. Norm Development

A. Bans and Moratoria

1. **Pass and enforce an international convention that establishes a moratorium on the development, export, and/or deployment of spyware.** A moratorium is a temporary ban on spyware, creating the time and space for further development of international regulatory frameworks and norms on spyware use while limiting the immediate harms of the rapidly evolving technology. A moratorium could be established through an international, legally binding treaty or other commitment among nations.
    - *Examples:* In April 2022, Costa Rica called for a global spyware moratorium, making it the first country to do so. In 2021, 156 civil society organizations and 26 independent experts published a joint open letter calling for states to implement a moratorium on surveillance technology in July 2021. UN experts also called for a moratorium on the sale of "life threatening" surveillance tech in August 2021. In May 2023, over 70 civil society organizations, journalists, and spyware experts signed a statement calling for countries to "implement an immediate moratorium on the export, sale, transfer, servicing, and use of digital surveillance technologies, as well as a ban on abusive commercial spyware technology and its vendors."
2. **Permanently ban the development, production, sale, export, and use of spyware technologies through an international convention.** A permanent ban on spyware would likely utilize many similar legal pathways to a moratorium but would be permanent.
    - *Example:* The Ottawa Treaty banning antipersonnel mines could be used as a model for an international ban on harmful technology.

B. Sanctions, Oversight, and Export Controls

1. **Strengthen international coordination through an international, shared sanctions regime against problematic spyware firms.** One path to such a regime is multilateralizing and expanding the U.S. Entity List to international venues to sanction malicious spyware companies. The U.S. Entity List is a trade restriction list that includes certain foreign entities subject to individualized import/export rules. The list does not establish embargoes on the companies included – it requires American companies to get a license to export or import products from the listed entity. Spyware groups currently on the U.S. Entity List include NSO Group, Candiru, Positive Technologies, Cytrox, Intellexa, and COSEINC, among others. The international community could multilateralize the Entity List to enact coordinated sanctions against spyware companies.
2. **Build an international human-rights-respecting regulatory framework for spyware.** Efforts to develop global norms against the use of spyware could include formal requirements and non-binding resolutions through the United Nations and other multilateral institutions on spyware development, export, and use.
    - *Example:* The UN General Assembly adopted a resolution affirming privacy rights for internet users and electronic communications in 2013, and the UN

High Commissioner for Human Rights Michelle Bachelet made a statement in 2021 emphasizing "the urgent need to better regulate the sale, transfer and use of surveillance technology and ensure strict oversight and authorization."

- *Example*: The OECD Guidelines for Multinational Enterprises establish corporate responsibility guidelines related to human rights, environment, employment, consumer protection, taxation, and competition. The OECD Guidelines have been adopted by 38 OECD members and 13 non-OECD governments.

3. **Improve international standards on surveillance, intelligence, and policing oversight to address spyware harms.** In keeping with existing resolutions and policies, standards could include more robust domestic guardrails to protect privacy rights and freedom of expression. These international standards could be developed and passed through multilateral international bodies like the United Nations, European Union, or African Union, or through an ad hoc multi-state coalition.
    - *Example:* In the European Union, Regulation 2021/821 governs dual-use exports and allows the E.U. to establish export controls in "sensitive and new emerging technologies." In March 2022, the European Parliament established a committee to study Pegasus and other surveillance spyware, including an explicit investigation into the "the alleged failure of Member States to act in respect of the involvement of entities in the E.U. in the development dissemination, or financing of the Pegasus and equivalent surveillance spyware… in so far as it is in breach of Union law, including Regulation (E.U.) 2021/821."
4. **Expand global sign-on to existing principles on the use of surveillance technologies and spyware.** Existing principles and guidelines on the use of spyware could be expanded to additional countries and leveraged to persuade countries to take more action against spyware harms.
    - *Example:* The Guiding Principles on Government Use of Surveillance Technologies and the Code of Conduct developed within the Export Controls and Human Rights Initiative were unveiled at the 2023 Summit for Democracy. The Guiding Principles have been endorsed by 11 countries thus far and commits signatories to establishing guidelines to spyware use in their respective countries, preventing export of spyware to malicious actors, sharing information on commercial spyware, working with corporate actors on spyware harm mitigation, and expanding partnerships for spyware accountability.
5. **Ensure transparency around the export of spyware and spyware-related products.** Global export and use norms for spyware technology can include ongoing human rights due diligence and impact assessments, including reviews by independent, expert third parties, to identify and prevent the human rights risks that arise from their tools and services. Reports on spyware license applications and exports could be mandated from spyware companies by states or international law.
6. **Expand global cybercrime coordination efforts and focus on spyware**. A centralized international organization on cybercrime, spyware, surveillance, and other related issues could lead research and policy efforts related to spyware accountability and boost technical capacity. An international cybercrime effort focused on spyware could be

hosted at the United Nations or a similar multinational organization in an effort to improve global coordination on fighting spyware.
    - *Example:* INTERPOL's cybercrime division or Europol's European Cybercrime Center could be useful examples of similar entities.
7. **Establish a spyware-specific committee at the United Nations.** The creation of a spyware-focused equivalent body to the UN Intergovernmental Panel on Climate Change (IPCC) could create a venue for the exploration of the use of spyware and for policy development to address spyware harms. A similar effort could be pursued within regional bodies instead of or in addition to a UN body.

C. Norm Development

1. **Strengthen international norms for democracy and human rights.** Stronger international norms for democracy and human rights could support the passage and enforcement of international agreements around spyware accountability.
2. **Build stronger global export and use norms and rules for spyware technology.** The global community can strengthen export norms and rules to prevent the sale of spyware to states that are likely to use spyware in violation of international human rights law. The UN can facilitate this process by developing resolutions and non-binding legal documents with UNHCHR and other international bodies to strengthen export and use norms. International bodies like the E.U. could establish stronger export regulations by implementing more robust regulations on the export of surveillance technology by companies in their jurisdictions. Additionally, although the Wassenaar Arrangement currently includes some "Intrusion Software" and "IP Network Surveillance Systems" export controls, stronger global norms around spyware technology could increase the effectiveness of the Arrangement and potentially expand its effects to non-member states. Building stronger international norms against the export and use of spyware can be facilitated through formal rulemaking institutions as well as informal communications between states.
    - *Example:* The European Union's investigation of Greece's granting of export licenses to Intellexa to export Predator spyware to Sudan could pose an opportunity to enforce the E.U.'s export regulations and impose consequences for spyware exports. This could potentially strengthen rules and norms against spyware technology.
3. **Establish a global norm on responsible vulnerabilities disclosure by national governments.** National governments could collectively establish clearer global norms around disclosing when they discover vulnerabilities in products that could be exploited by spyware technology. These norms would improve the national vulnerabilities disclosure processes discussed elsewhere in this document.
4. **Create a universal declaration of digital human rights and include protection from commercial spyware as a key right.** Modeled after the Universal Declaration of Human Rights, a declaration of human rights focused on digital rights could influence future hard and soft law around spyware and other surveillance-related topics.

III. Mechanisms of Change: Investor Engagement

Overview

Spyware firms rely on several inputs to develop, sell, and deploy their products, most notably capital. One method of limiting the harms of spyware is to weaken or cut off streams of funding to spyware firms. Venture capitalists, public and private investors, and media organizations all have roles to play in this set of strategies by making it more difficult for spyware companies to find capital, encouraging investors to divest from companies perpetuating spyware harms, and deterring potential investors from becoming involved in the spyware industry. Potential levers of accountability include:

1. **Establish human rights criteria within investor legal compliance processes.** Including the essential elements of human rights due diligence in a pre-investment screening and risk assessment process can help investors shield themselves from legal and financial risk while disincentivizing private investment into spyware and other related tools.
2. **Voluntarily divest from investments in spyware and spyware-related industries.** Spyware and other related industries hold significant financial risk for investors, which could incentivize investors to divest from spyware-related holdings voluntarily. Widespread and explicit divestiture could signal to would-be spyware company founders that it will be difficult to attract funding.
3. **Civil society organizations can educate venture capitalists and other investors on the harms and risks associated with spyware.** Civil society organizations could publish reports for investors and other parties related to the spyware industry on best practices for evaluating the potential harms of their involvement with certain spyware, surveillance, and technology companies**.** Due diligence guides, best practices, and other similar reports can guide investors who may not consider human rights violations as a part of their risk evaluation. Educating this key constituency could help prevent funding from entering the surveillance and spyware industry.
    - *Example:* The Surveillance Technologies Accountability Project, a joint initiative of Access Now, Business & Human Rights Resource Centre, and Heartland Initiative, published a human rights due diligence guide for investors in the surveillance technology ecosystem.
4. **Public media campaigns can pressure investors to divest from spyware companies.** Public naming and shaming of investors in spyware technologies can pressure them to pull funding from spyware companies and spark similar divestment in other jurisdictions.
    - *Example*: In 2021, a number of news articles were published revealing the State of Oregon's investments in NSO Group. In March 2022, labor organizers in the state called for the state pension fund to divest from the investment fund that owned NSO Group.
5. **Engage investor trade associations to establish best practices and collectively commit investors to not funding spyware and related technology.** Trade associations and other

industry forums could be fruitful arenas for collaboration on education about spyware harms, development of shared principles or best practices, and collective commitment to spyware accountability.

6. **Work with ESG data firms to ensure spyware investments receive poor marks.** Economic, Social, and Governance (ESG) investing has grown tremendously in recent years. However, many ESG data firms and index providers do not adequately integrate digital and surveillance harms into their scoring. If investments that can fund spyware or surveillance consistently receive lower scores, it could reduce the flow of funds to spyware companies.

IV. Mechanisms of Change: Corporate Action

Overview

The wide array of technology companies whose products are vulnerable to becoming a vehicle for spyware play a key role in deterring the production and use of spyware and holding spyware companies accountable for the exploitation of their consumers. Internet service providers (ISPs), social media companies, device developers and manufacturers, search and internet navigation platforms, and other technology companies all have incentives for their consumers and user data and communication to be safely stored and managed and for their products to be protected from hacking and other vulnerabilities.

Corporate action includes two main categories of levers:

A. **Data Security & Analysis**
B. **Other Approaches**

A. Data Security & Analysis

1. **Continue to develop new security features for products, platforms, and data repositories.** Technology companies can help secure their products against spyware attacks by continuing to investigate vulnerabilities and creating new security features and capabilities. Features could include strong encryption, robust data storage and transfer security, and data minimization options.
    - *Example:* Apple's development of "lockdown mode" and Samsung's "Message Guard" aim to protect consumer devices. Microsoft's Sentinel program and the Threat Intelligence solution from the Microsoft Sentinel Content Hub facilitate the detection and discovery of spyware on Microsoft products.
2. **Take voluntary action to commit to stronger investigation of spyware use on their products, notification to users when products are compromised, and data minimization provisions.** Service providers could commit to stronger and faster notification of users when products are compromised and decrease the data that they collect, transfer, and store to minimize the risk and impact of compromised data. Companies developing and producing tracking equipment could publish and follow an

industry standard allowing platforms to incorporate physical tracking detection capabilities on mobile apps and operating systems and could eschew "invisibility" features that allow their products to be undetectable.

3. **Publish analyses of the impact of spyware on their products and establish guidelines for spyware detection and solutions.** Naming and shaming spyware actors can deter harmful behavior and share crucial information with civil society and the public at large. It also serves to support public awareness of spyware issues.
    - *Example:* Microsoft published a report on QuaDream with Citizen Lab, outlining the technical investigation that led to the exposure of the malware, detailing the vulnerabilities that the spyware exploited and outlining prevention procedures and detection indicators.
4. **Utilize trade associations as forums for creating and signing onto industry-wide standards mitigating spyware harms.** Trade associations and their constituent companies could encourage the establishment of standards on product and data security, promote stronger investigation of spyware use and vulnerabilities, and establish industry-wide best practices for disclosure and transparency.
    - *Example:* The Cybersecurity Tech Accord announced a set of industry principles in March 2023, with signing companies committing to: "take steps to counter cyber mercenaries' use of products and services to harm people; identify ways to actively counter the cyber mercenary market; invest in cybersecurity awareness of customers, users and the general public; protect customers and users by maintaining the integrity and security of products and services; and develop processes for handling valid legal requests for information."

B. Other Approaches

1. **Advocate for spyware protections for consumers and other national legislation levers of accountability.** Technology companies can help promote the actualization of national legislation levers through advocacy and public support of accountability measures.
2. **Build stronger relationships and cooperation with civil society groups and digital security researchers to detect and address vulnerabilities exploited by spyware.** Companies could devote more resources to identifying spyware and ensuring that services are secured against exploitation, working with civil society groups with technical expertise to investigate potential vulnerabilities and system failures. ISPs and technology companies could increase transparency and share more information with civil society organizations to address spyware exploitation. Efforts in this strategy could also directly support capacity at relevant civil society organizations.
3. **Establish restrictions on access to products for individuals involved with spyware abuses, including employees of spyware production companies.** Blocking employees of spyware companies from platforms could help deter people from joining spyware companies, disrupting the talent pool for the industry.
    - *Example:* Facebook deleted the accounts of NSO Group employees in 2019 after WhatsApp, a Facebook-owned company, sued NSO Group. WhatsApp claimed

that the NSO Group employees were calling victims from their personal WhatsApp accounts to infect them with spyware. Facebook's lawsuit against NSO Group included seeking a permanent junction of all NSO employees from "accessing or attempting to access" Facebook's services.

4. **Strengthen formal channels of communication and cooperation between corporations to address spyware challenges and harms.** Global technology companies could cooperate at an official forum to share best practices, learnings, and challenges related to addressing spyware challenges and harms as well as to strategize on the coordinated execution of other corporation action levers.
    - *Example:* The Cybersecurity Tech Accord brings together global technology companies to cooperate on cybersecurity issues. The Cybersecurity Tech Accord publishes case studies, hosts events, commits signatories to policies, and provides a forum for cooperation across the industry.
5. **Contribute resources to technical labs doing forensic investigation on spyware abuses.** Technology companies could provide monetary support as well as technical assistance and human capital to technical labs investigating spyware use and harms.
6. **Engage additional stakeholders.** Some technology companies whose products have been unwittingly involved in spyware abuses (for example, Apple and WhatsApp) have fought back against spyware manufacturers. However, engaging a larger number and wider range of corporate actors to act against spyware use could increase pressure on spyware companies and help promote the implementation of spyware accountability policies and regulations. Additional companies to engage in anti-spyware activities could include ISPs (which facilitate the networks through which spyware companies operate), cloud storage providers (where data targeted by spyware companies is often stored), and others.

V. Mechanisms of Change: Strategic Litigation

Overview

Strategic litigation against spyware companies, financiers, and states that deploy spyware against its citizens can stop future of uses of spyware products, penalize bad actors involved with spyware harms, bring restitution to victims, establish precedence for future spyware-related litigation, bankrupt spyware companies, and strengthen deterrent forces for potential skilled employees and funders of spyware companies. Strategic litigation also works in conjunction with campaign and media levers to educate the public on spyware harms and bring spyware into the public eye. Key challenges to litigation-based strategies include challenges with jurisdiction, sovereign immunity, difficulties with gathering evidence, and lack of precedent. Additionally, the extended timeline for litigation combined with spyware companies' ability to disband and regroup elsewhere limits possibilities for accountability as specific spyware companies may have created a different legal entity by the time legal cases are completed.

Strategic litigation includes two main categories of levers:

A. Direct Litigation

B. Litigation & Related Field Support

A. Direct Litigation

1. **Victims of spyware attacks can sue spyware providers, states that use spyware, and funders of spyware technology for direct harm.** Journalists and other human rights activists who are directly impacted by the harms of spyware could mount legal campaigns to challenge governmental uses of spyware technology through multiple avenues in partnership with civil society organizations with the technical expertise to build evidence in legal cases. Victims can press for investigations in countries of proliferation, bring lawsuits before international bodies like the European Court of Human Rights, and band together for class action lawsuits.
    - *Example:* 15 employees of El Faro, a Salvadoran news organization sued NSO Group in United States court in December 2022, arguing that the firm violated the Computer Fraud and Abuse Act, among other laws. The suit was filed by The Knight First Amendment Institute at Columbia University.
    - *Example:* The Hungarian Civil Liberties Union sued NSO Group in the European Court of Human Rights and pushed for an investigation against NSO Group in Israeli on behalf of six human rights activist and journalists in January 2022.
2. **Tech companies can sue spyware companies for harm to their platforms or products and provide legal support to other victims who are suing spyware companies.** In addition to directly suing spyware companies themselves, technology companies can support litigation efforts by other actors by filing amicus briefs or providing legal and technical expertise in support of spyware victims.
    - *Example:* In 2021, Apple sued NSO Group for its surveillance of Apple users and sought a permanent injunction banning NSO Group from using Apple products or services. WhatsApp is also pursuing a lawsuit against NSO Group.
3. **Users can sue technology companies whose platforms and devices' vulnerabilities are exploited by spyware programs.** In addition to suing spyware producers, victims of spyware harms can sue the technology companies that gather and store their data for the vulnerabilities that exposed them and their data to targeting by spyware. Lawsuits can include claims for accessing user content without authorization, breaking promises outlined in terms of use or other policy statements, and copyright or other content related claims.
    - *Example:* Three Facebook and iOS users are bringing two class action lawsuits against Meta on behalf of all iOS users impacted, claiming that the company left users vulnerable to surveillance and tracking by covering up privacy risks, ignoring iOS user privacy choices, and collecting data on third-party websites viewed through in-app browsers.

B. Litigation & Related Field Support

1. **Establish a precedent for suing financiers for enforcement purposes and funds for victims.** Strategic litigation against financers of spyware companies could, if successful, establish a precedent allowing victims to gain compensation from winning spyware abuse cases and help create enforcement policies against spyware companies. Litigation against spyware investors could also deter funding for spyware companies.
2. **Fund more research on effective spyware litigation strategies.** Learning from success and failures in the spyware litigation space could help identify best practices for holding spyware companies, tech companies, and states accountable for spyware abuses.
3. **Develop and distribute a guidebook for victims on how to pursue litigation**. Civil society organizations and legal entities supporting strategic litigation efforts can create and publish guidebooks on how to navigate the legal landscape around spyware, build an evidence base, and gather support from existing resources.
4. **Utilize the discovery stages of litigation to support forensic investigators and technical labs.** Litigators pursuing legal action can use the discovery stage of lawsuits and other legal mechanisms to force spyware firms to share key technical markers and knowledge that could support forensic investigators who are exploring potential spyware cases.

VI. Mechanisms of Change: Technical Interventions

Overview

Technical action is the discovery, investigation, and reporting of spyware use and harms. Civil society organizations with technical expertise to detect, investigate, and publish reports on the use of spyware to harm organizations and individuals are crucial to limiting the development and use of spyware. A key challenge to technical interventions is the inherent information asymmetry between spyware developers and organizations conducting forensic analysis. When organizations publish their forensic findings and share their patches and methods of detection publicly, spyware developers can then improve their product to skirt those findings. Civil society organizations, however, cannot learn from the findings of spyware producers, leaving them perpetually in a defensive or reactive posture. Despite this challenge, technical interventions remain key to the work of holding spyware companies and users accountable, as media and communications efforts as well as litigation are largely dependent on technical action to reveal cases of spyware deployment and build a case against spyware producers and deployers. Specific levers to drive change include the following:

1. **Investigate existing or potential malicious usage of spyware.** Organizations like Amnesty International and Citizen Lab search for evidence of spyware use and harm

against journalists, human rights activists, and other vulnerable populations, using forensic investigatory tools to uncover malicious uses of spyware.

- *Example:* Amnesty International's "Forensic Methodology Report: How to catch NSO Group's Pegasus" outlines the organization's methodology and technical indicators for detecting the use of spyware.

2. **Develop innovative new tools to detect and investigate the use of spyware.** Established organizations investigating spyware uses can develop toolkits, forensic tools, and other resources to help less well-resourced organizations to contribute to the investigation of spyware abuses. A key challenge to this lever is the method of ensuring the continued utility of new tools, as spyware producers can access public investigation materials and learn from them to better conceal their products.
    - *Example:* Tools like the Mobile Verification Toolkit (MVT) published by Amnesty International and developed to detect the use of Pegasus, help civil society organizations discover and report on abuses of spyware while packaging methodologies for potential reproduction with other spyware products. MVT is a tool that simplifies the process of acquiring and analyzing data from Android devices and facilitates the analysis of records from iOS backups and file system dumps, specifically to identify potential traces of compromise.
3. **Expand offensive approaches to cyber defense.** National security or intelligence entities, as well as federal actors could take offensive action to attack and undermine foreign spyware firms. Such actions could also include technical efforts to disable web infrastructure hosting or other products facilitating spyware.
    - *Example:* The U.S. Federal Bureau of Investigation infiltrated the "Snake" malware network, a Russian cyberespionage system, by infecting a computer in the United States to infiltrate and turn the malware network against itself. Offensive action against foreign spyware companies and products could prevent future attacks.
4. **Create, expand, or improve bug bounty programs to identify vulnerabilities contributing to the global zero-day exploit market**. Zero-day exploits take advantage of vulnerabilities in a product. Bug bounty programs provide rewards to skilled hackers to catch these vulnerabilities before malicious actors can use them and incentivize people with strong technical knowledge to work for technology companies rather than spyware companies. Although bug bounty programs have mixed efficacy, responsible approaches to bug bounty programs, potentially through small open-source programs like the Sovereign Tech Fund's Bug Resilience Program, could support efforts to identify and patch vulnerabilities.
5. **Expand civil society and security technologists' capacity to better monitor and circumvent spyware by funding the expansion of current efforts or the establishment of more entities with technical expertise.** Many interviewees pointed to Amnesty International and Citizen Lab as the primary actors with the technical expertise to discover and investigate spyware abuses. Expansion of capacity in this area could enable more litigation to hold bad actors accountable, facilitate more communications campaigns to raise the profile of spyware abuses, and augment deterrence factors for

spyware companies, employees, and funders. Increased funding for research to detect and uncover targeted espionage using a variety of networking, monitoring, and other investigative techniques can provide the foundation for the execution of other key levers.

6. **Expand preventative measures for parties that are at risk of becoming victims of spyware attacks.** Civil society organizations with technical expertise and technology companies could cooperate with human rights organizations, journalists, and activists to provide them with preventative security tools, education on how to better protect themselves from spyware attacks, and identification factors for malicious spyware.
7. **Standardize documentation of spyware cases.** Actors working on technical documentation and evidence collection for spyware cases could standardize the documentation and public reporting of technical details to better share findings and collect best practices.
8. **Improve geography, investor, and corporate structure mapping of spyware producers and malicious users.** Through forensic analysis and other corporate and investor mapping strategies, mapping and investigation of spyware-involved actors could strengthen spyware accountability efforts generally by directing civil society towards the most strategic targets. Litigation efforts are particularly highly dependent on forensic investigation and the identification of spyware producers, funders, and users. Additionally, mapping of the entire spyware supply chain, including corporate structures, shell companies, third party resellers, and investors could help civil society organizations and other stakeholders focus attention on geographic areas and entities with an influx of spyware.

VII. Mechanisms of Change: Media & Education

Overview

Media and education efforts to raise public knowledge and awareness of spyware harms can be a valuable tool for pressuring spyware companies and state actors into taking measures toward commercial spyware accountability. By exposing the harms of spyware to individuals and communities, effective media and education campaigns can name and shame bad actors, deterring individuals from joining organizations that develop or use commercial spyware, discouraging the use of spyware by organizations and states, and bringing more resources to efforts to expose and hold bad actors accountable.

Specific levers to drive change include:

A. Deterrence Campaigns
B. Education Campaigns

A. Deterrence Campaigns

1. **Publish reports and news stories about the harms of spyware and name bad actors in the industry to deter engineers from working with spyware tech companies.** Public

naming and shaming of spyware companies can deter skilled workers from working for spyware companies, persuade current employees to quit, and influence employees at spyware companies to leak information about spyware use.

2. **Investigate and publish reports on the financing of spyware companies.** Public reporting aimed at naming and shaming investors in the spyware industry can deter investors from future involvement with spyware companies. A similar approach could include developing reports highlighting investors' policies (or lack thereof) regarding investments in spyware companies.

B. Education Campaigns

1. **Increase public education and awareness about spyware harms and victims by publishing news media and reports.** Support media efforts by investing in communications to publish the stories of victims and push the issue of spyware into the public consciousness, utilizing effective symbols and stories. Local-language media in countries where spyware companies proliferate can be particularly effective in pressuring states and spyware companies to adopt spyware limitations. Public resources and media can also help members of the public develop greater technical literacy and spread measures for good internet and data privacy practices.
    - *Example:* The public release of the Pegasus Project report sparked an active global news cycle about spyware and the threats that journalists face as a result of the use of spyware technologies. This publicity has brought spyware into the public consciousness and has arguably paved the way for much of the progress toward spyware accountability since 2021.
2. **Educate potentially affected communities, organizations, and individuals on the risks of commercial spyware.** Publish public reports on ways to prevent, detect, and report the use of commercial spyware and private surveillance technology for organizations involved with journalism, political party organization, political protest, and other vulnerable populations.
3. **Fund civil society to further research and increase public education on the harms of spyware and stalkerware.** Further research on the prevalence of spyware, stalkerware, and technology-facilitated intimate partner violence, abuse, and harassment can better inform future efforts toward accountability and prevention.
4. **Collaborate across media actors to maximize multiple levels of impact.** Journalists and other media actors covering spyware cases could cooperate to document cases and maximize impact locally, nationally, and internationally. The Pegasus Project was an initiative in this model.
5. **Activate national security and intelligence leaders as advocates for spyware accountability.** Stakeholders in the military, national security, and intelligence communities can serve as trusted messengers with unique reach in campaigns for spyware accountability. These voices can help overcome national security objections to reining in spyware.

6. **Pursue a campaign to expand spyware language and awareness outside the privacy framework to address the citation of terrorism and national security claims to legalize spyware use.** Nations sometimes utilize claims of terrorism prevention and national security to justify the use of spyware against their citizens. International recognition and undermining of the legitimacy of these claims through exposing the harms of spyware could help facilitate accountability. Additionally, a campaign to link the legal framework of human rights to spyware harms and other human rights abuses like forced disappearances and extrajudicial killings could move spyware accountability initiatives forward.
7. **Provide support for the mental and physical health and security of activists working to advance spyware accountability.** Activists and other stakeholders working to advance spyware accountability are at a unique risk of physical and digital attacks from private and governmental actors. Protection from physical risk and support for mental and emotional needs could help stakeholders sustainably support efforts towards spyware accountability.

A Note on Stalkerware

Spyware is far from the only category of technology driving surveillance-related harms. Stalkerware, according to the Coalition Against Stalkerware, is a category of "tools – software programs, apps and devices – that enable someone to secretly spy on another person's private life via their mobile device." Some experts have suggested commonalities in the harm and accountability strategies of spyware and stalkerware technologies: both technologies involve illicit access to victims' personal data and often operate without obvious identifying activity, making it difficult for victims to recognize that they are being monitored.

Despite similarities in technology, however, there are notable differences in the political and legal harms structures occupied by spyware and stalkerware. Stalkerware is much more accessible to the public, as the target user is private individuals rather than states. Stalkerware is often employed by domestic violence or intimate partner violence offenders and perpetrators. While laws generally exist to protect victims of stalkerware, the challenge often lies in the practical enforcement of those laws, rather than the lack of legal precedent that is often seen in commercial spyware cases. Stalkerware cases are also less likely to face jurisdictional challenges.

Potential areas of focus for levers *unique to* stalkerware include:

- Content moderation-related levers to stop private individuals from accessing stalkerware products online.
- Exposing companies that permit stalkerware product advertising.
- Promoting or providing technical support for survivors and victims of spyware, as well as technical training for those working with impacted communities.
- Educating law enforcement officials on how to identify and prosecute stalkerware cases.

However, several spyware accountability levers outlined in this report could also be applied to stalkerware cases. Since spyware and stalkerware both utilize vulnerabilities in platforms, websites, or devices, technology companies can help mitigate both spyware and stalkerware risks by addressing these vulnerability types. Other areas of intersection may include:

- Levers deterring the flow of human and financial capital to spyware companies could also apply to stalkerware companies in some cases.
- Public education about the harms of spyware and stalkerware can help reduce the stigma of victimhood and increase public knowledge about ways to detect remote monitoring. Public awareness of companies funding these products can also mobilize consumer awareness and action.
- Incentivize people who may be motivated to work for stalkerware or spyware companies to instead work for teams working against the development and scale of these tools.

Conclusion

Freedman Consulting, LLC, is honored to work on behalf of the Ford Foundation and the Open Society Foundations in this crucial work to hold oppressors accountable for the personal and political harm perpetuated by spyware technology. The rise of commercial spyware threatens democracy, journalists, activists, human rights defenders, and everyday citizens around the world. We hope that this document provides stakeholders with an illustrative menu and cohesive taxonomy for future discussions and collaborative efforts toward holding spyware producers and users accountable to the public interest.

Acknowledgments

The authors would like to acknowledge the contributions of the many spyware experts whose input made this report possible. We thank the Ford Foundation and Open Society Foundations for supporting this research, as well as the program staff at these foundations who informed the direction and scope of this research. Alondra Solis and Sofia Rhodes also contributed to this report. Finally, the research and efforts of Citizen Lab, Amnesty International, Access Now, David Kaye (and participants in workshops organized at the UC-Irvine School of Law's International Justice Clinic), Steven Feldstein, and many others were crucial to this report and to the ongoing efforts toward spyware accountability worldwide.

This document is intended as a brief, non-exhaustive proposed framework and taxonomy meant to spark further discussion on tools and pathways towards spyware accountability. Any errors in this document are the authors' alone and should not be taken to reflect upon other contributors.

About the Authors

Freedman Consulting

Freedman Consulting, LLC, works on a broad portfolio of issues focused on innovations for the greater social good, finding smart solutions to your most challenging problems. We use our diverse experience in philanthropy, politics, public policy, nonprofits, journalism, and communications to advise a broad range of clients advancing the public interest. We have worked with the country's top policymakers, largest foundations, leading advocacy groups, and other public interest leaders as partners in change. Our approach focuses on helping clients define their goals and develop comprehensive approaches that flexibly respond to client needs.

Alexander Hart, Vice President

Alexander C. Hart is a Vice President with Freedman Consulting, LLC, where he manages projects in policy and strategic planning, research, communications, public opinion, evaluation, and event facilitation. His work for firm clients covers a broad portfolio of issues, including technology policy, poverty and economic opportunity, democracy, and municipal innovation.

Kennedy Patlan, Project Manager

Kennedy Patlan is a Project Manager at Freedman Consulting, LLC, where she assists with strategic development, project management, and research. Her work covers technology policy, health advocacy, and public-private partnerships.

Rachel Lau, Senior Associate

Rachel Lau is a Senior Associate at Freedman Consulting, LLC, where she assists project teams with research, strategic planning, and communications efforts. Her work covers a range of issue areas, including technology policy, criminal justice reform, economic development, human rights, and diversity and equity efforts.

Appendix: Research Methodology Details

This report seeks to provide a menu of levers to advance spyware accountability and establish a taxonomy for understanding levers to advance spyware accountability.

To develop this report, Freedman Consulting interviewed thirteen spyware accountability experts to surface insights about high-level approaches to mitigating harms from spyware and related tools, like stalkerware. Interviewees included human rights lawyers, journalists, experts at civil society organizations, technical professionals, and academic experts, among others.

To supplement interview findings, Freedman Consulting also conducted a research scan primarily on the United States and Europe on both policy and non-policy levers from media sources and relevant stakeholders. The research scan was constrained to sources dating back to 2018 with a focus on levers of accountability. Initial research began with scans of major news media and technology-specific news sources as well as the online publishing arms of relevant stakeholders. Sources included:

- *The New York Times*
- *Washington Post*
- *Ars Technica*
- *The Verge*
- *Cyberscoop*
- *Al Jazeera*
- *Haaretz*
- *Social Science Research Network*
- *Wall Street Journal*

The following stakeholders' online publishing arms were also scanned for relevant reports on spyware accountability levers:

- Amnesty International
- Access Now
- Coalition Against Stalkerware
- Citizen Lab
- CyberPeace Institute
- Carnegie Endowment for International Peace
- Electronic Frontier Foundation
- Freedom House
- Human Rights Watch
- Knight First Amendment Institute at Columbia University
- National Cybersecurity Alliance
- Safety Net Project

Iterative research was conducted throughout the interview process to investigate new areas of inquiry.