Atlantic Council
CYBER STATECRAFT INITIATIVE

# 404 Accountability not found:

## Spyware accountability through software liability

Sara Ann Brackett and Jen Roberts

Atlantic Council

CYBER STATECRAFT INITIATIVE

The **Cyber Statecraft Initiative** works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.



Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2025

## Authors

Sara Ann Brackett

Jen Roberts

## Acknowledgments

This report would not have been possible without the support of the Spyware Accountability Initiative and the pro bono research assistance provided by Christopher Hart and his team at Foley Hoag LLP, Langie Cadesca, Katherine Jung, and Gilleun Kang. Thank you to Nikita Shah and Trey Herr, as well as other colleagues at the Cyber Statecraft Initiative for their support, guidance, and reviews of this research. Thank you to Lisandra Novo and Chinmayi Sharma for their review of a draft of this work. All errors are the authors' own.

# Table of contents

# Executive Summary

The global spyware market enables human rights harms and amplifies national security risks. Despite mounting awareness of spyware abuses and repeated efforts to pursue accountability through litigation, existing legal avenues to accountability have proven inadequate at delivering justice or compensation for affected individuals.

This report identifies four obstacles that frustrate accountability efforts: limited awareness among targeted individuals of their compromise, the intentional obscurity of spyware vendors that engage in name changes and jurisdictional arbitrage, difficulties establishing proper legal jurisdiction, and risks of exposing valuable threat intelligence during litigation proceedings.

Technology companies operating messaging platforms and mobile operating systems possess unique capabilities that position them as essential actors in accountability efforts. These capabilities include unmatched technical insights for detecting and attributing spyware infections, established relationships with users that facilitate threat notifications, exclusive ability to patch vulnerabilities and secure products against exploitation, and resources to develop opt-in enhanced security features for high-risk users.

This report proposes a legislative safe harbor framework that would incentivize technology companies to engage in spyware accountability by shielding compliant firms from litigation related to software insecurity, including potential products liability claims. Under this framework, companies would qualify for protection by meeting standards of behavior including comprehensive threat notification and detection programs, responsible information sharing with researchers and advocacy organizations, provision of enhanced security features, and rapid remediation of identified vulnerabilities. This approach recognizes both the heightened threat environment companies face when defending against state-sponsored actors and the rapidly evolving nature of spyware capabilities that requires flexible regulatory responses.

By aligning incentives to reward proactive security measures rather than penalizing failures, this safe harbor structure could incentivize prevention and protection for spyware while complementing existing accountability approaches. The framework acknowledges that perfect security against well-resourced, nation-backed actors is not technically feasible or economically reasonable, but encourages meaningful investment in best practices that have proven effective in mitigating spyware harms.

# Introduction

Spyware is a type of malicious software that facilitates unauthorized remote access to an internet-enabled target device for purposes of surveillance or data extraction.[1] More than 80 countries are reported to have procured spyware and used it against individuals.[2] In some cases, states have used spyware for intelligence and law enforcement purposes. In many cases, targets include journalists, political opposition, lawyers, academics, ethnic or religious minorities, businesses, and activists.[3] Spyware vendors are entities that develop, support, and sell spyware to end users.[4] Often, resellers, brokers, and intermediaries play a role in connecting vendors to customers, including government customers.[5] While vendors may have varying degrees of control over the use of their spyware tools after purchase, at least some vendors are responsible for the installation, delivery, and continued operation of spyware capabilities.[6]

Despite repeated efforts, court action has offered limited recourse to affected individuals pursuing accountability from spyware harms. Through the pursuit of court action, individuals often seek compensation for the harms of spyware that they have suffered and to prevent similar harms to others. Alarmingly, according to a tracker of spyware-related litigation maintained by Citizen Lab no case in the United States or the United Kingdom brought by victims has achieved final resolution against a spyware vendor.[7] By contrast, technology companies have seen slightly greater success in lawsuits against spyware vendors, seeking justice for the harms of spyware suffered by their businesses and seeking to prevent further harm from spyware companies to themselves and their customers. WhatsApp's case against NSO Group achieved an eye-popping $167 million judgement from a jury in the Northern District of California, but as of September 2025, litigation in the matter is ongoing.[8] Cases against spyware vendors take years—WhatsApp's decision in May is the result of a suit originally filed in October 2019.[9] Meanwhile, spyware vendors continue to emerge and evolve, perpetuating abuses against individuals and developing new exploits against messaging apps, mobile operating systems, and other popular consumer products.[10]

Efforts to constrain spyware's impact include multilateral efforts to counter the proliferation of offensive cyber capabilities, visa bans on individuals involved in the development and sale

1. Jen Roberts et al., *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*, *Atlantic Council,* September 4, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.
2. Ellen Nakashima and Tim Starks, "At Least 50 U.S. Government Employees Targeted with Phone Spyware Overseas; White House Bans Federal Agencies from Using Spyware That Poses National Security and Human Rights Risks in the U.S.," *Washington Post*, March 27, 2023, https://www.washingtonpost.com/national-security/2023/03/27/spyware-diplomats-us-pegasus; Andy Greenberg and Lily Hay Newman, "US Congress was Targeted with Predator Spyware," *Wired*, October 14, 2023, https://www.wired.com/story/us-congress-spyware.
3. Jen Roberts et al., *Markets Matter: A Glance into the Spyware Industry*, *Atlantic Council*, April 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/markets-matter-a-glance-into-the-spyware-industry/.
4. Roberts et al. *Mythical Beasts and Where to Find Them*.
5. Sarah Graham, Jen Roberts, and Nitansha Bansal, *Mythical Beasts: Diving into the Depths of the Global Spyware Market*, *Atlantic Council*, September 10, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/.
6. Suzanne Smalley, "Testimony from NSO Group Raises Questions about its Culpability for Spyware Abuses," *The Record*, November 19, 2024, https://therecord.media/nso-group-whatsapp-case-documents; Stephanie Kirchgaessner, "NSO - Not Government Clients - Operates its Spyware, Legal Documents Reveal," *The Guardian*, November 14, 2024, https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp.
7. Within this litigation tracker, this report is concerned with cases that are brought 1) in US or UK courts 2) against a spyware vendor (under the *Mythical Beasts* definition) 3) by a victim or company, which specifically excludes the September 2021 DarkMatter enforcement action brought by the DOJ and FBI; Siena Anstis, "Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry," *The Citizen Lab*, last updated August 15, 2025, https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.
8. WhatsApp Inc. et al. v. NSO Group Technologies Limited, et al., 4:19-cv-07123-PJH (N.D. Cal. 2025).
9. Joseph Menn, "Spyware Maker NSO Ordered to Pay for Infecting WhatsApp Accounts," *Washington Post*, May 6, 2025, https://www.washingtonpost.com/technology/2025/05/06/nso-pegasus-whatsapp-damages/; Asaf Lubin, "Unpacking WhatsApp's Legal Triumph over NSO Group," *Lawfare*, January 7, 2025, https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group.
10. Roberts et al., *Mythical Beasts and Where to Find Them*.

of spyware, and investigations into previous spyware use.[11] Recognizing the importance of international coordination and deconfliction to the success of any spyware accountability effort, the scope of this report's includes avenues towards spyware accountability through liability in both the United States and the United Kingdom. The two countries share somewhat compatible legal systems and host a significant number of the technology companies relevant to this spyware accountability framework. The two jurisdictions already host important legal cases related to spyware accountability.

Individuals affected by spyware have brought lawsuits in the United Kingdom and the United States against both spyware vendors and states using spyware, which has created a notable fork in jurisprudence between the two jurisdictions. In the United States, foreign states retain sovereign immunity in civil suits except under a specific set of circumstances outlined in the Foreign Sovereign Immunities Act.[12] In a case involving Ethiopia's use of the FinSpy spyware tool, the US District Court for the District of Columbia ruled that sovereign immunity prevented a suit brought by a US citizen residing in Maryland against the government of Ethiopia.[13] In the WhatsApp case against NSO Group, the US Court of Appeals for the Ninth Circuit held, and the Supreme Court declined to overturn, that sovereign immunity does not extend to NSO Group, even though the spyware vendor claimed to be acting as an agent of a foreign state.[14] Meanwhile, in the United Kingdom, courts have allowed cases against foreign states involving the use of spyware by Bahrain, Saudi Arabia, and the United Arab Emirates to proceed.[15] Taking into account the different approaches to cases against foreign states between the United States and the United Kingdom, the authors explore a policy solution that would be feasible in both countries, focusing on accountability for spyware vendors rather than state customers and perpetrators.

This piece examines obstacles to accountability, discussing why legal actions against spyware vendors have achieved limited results in compensating victims, imposing costs on spyware vendors, and creating deterrent effects. Spyware vendors engage in practices that frustrate paths to accountability, such as shifting identities, opaque corporate structures, and movement between jurisdictions. Individual victims of spyware, especially when targeted by powerful and well-resourced states, face steep costs in pursing legal recourse against spyware vendors and procedural challenges in showing causation and fault. In addition to the cost of litigation, individuals can suffer physical, financial, or other retaliation against themselves or their affiliates, including family, friends, colleagues, and healthcare providers.[16] On the other hand, technology companies can be disincentivized from litigation, as lawsuits against vendors are slow, difficult, expensive, and in some cases, could require exposure of detection techniques or sensitive design information and practices. This exposure could pose wider risks to the security and integrity of software products, while ultimately insufficiently discouraging vendors from engaging in the development and sale of spyware.[17]

The authors posit that technology companies have an essential role in the pursuit of accountability for spyware harms and abuse. Technology companies can provide technical insights, facilitate interactions with affected individuals, secure software, and provide opt-in enhanced security features to protect the most vulnerable users of messaging platforms and mobile devices. These capabilities can assist advocacy groups, civil society organizations, and individuals targeted by spyware in achieving accountability. To incentivize the use of those capabilities, this piece suggests a policy mechanism, a safe harbor, which would reward technology companies that engage in best practices for spyware accountability by shielding them from certain litigation related to spyware's harms, even when those harms are enabled by security flaws in their products. This safe harbor structure assists with existing challenges within the legal system that frustrate accountability efforts by encouraging technology companies to utilize their existing strengths. This approach would complement and strengthen additional approaches to accountability, while acknowledging the difficulties those approaches must overcome to achieve justice.

11. Roberts et al., *Mythical Beasts and Where to Find Them*.
12. Foreign Sovereign Immunities Act of 1976 (FSIA), Pub. L. 94-583, 90 Stat. 2891 (1976).
13. Luca Marzorati, "D.C. Circuit: Ethiopia Immune from Hacking Suit under the FSIA," *Lawfare*, March 21, 2017, https://www.lawfaremedia.org/article/dc-circuit-ethiopia-immune-hacking-suit-under-fsia; Nate Cardozo, "D.C. Circuit Court Issues Dangerous Decision for Cybersecurity: Ethiopia is Free to Spy on Americans in Their Own Homes," *Deeplinks (blog)*, March 21, 2017, https://www.eff.org/deeplinks/2017/03/dc-circuit-court-issues-dangerous-decision-cybersecurity-ethiopia-free-spy.
14. NSO Group Technologies Limited v. WhatsApp Inc., No. 21-1338, Supreme Court of the United States, petition for a writ of certiorari filed April 6, 2022 denied January 9, 2023, https://www.supremecourt.gov/docket/docketfiles/html/public/21-1338.html.
15. "Court of Appeal Rules that Two Bahraini Dissidents Can Bring FinFisher Spyware Claims Against the Kingdom of Bahrain in the UK," Leigh Day, October 4, 2024, https://www.leighday.co.uk/news/news/2024-news/court-of-appeal-rules-that-two-bahraini-dissidents-can-bring-finfisher-spyware-claims-against-the-kingdom-of-bahrain-in-the-uk/.
16. Stephanie Kirchgaessner, "Mexico NSO Spyware Journalists Human Rights Hacked Pegasus," *The Guardian*, October 4, 2022, https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus.
17. Suzanne Smalley, "Apple Seeks Dismissal of NSO Lawsuit over Pegasus Spyware," *The Record*, September 13, 2024, https://therecord.media/apple-seeks-dismissal-of-nso-lawsuit-pegasus-spyware.

# Obstacles to accountability

Spyware use harms individuals by targeting their communications, and technology companies, by hijacking their infrastructure and breaching their products. Accountability encompasses incentive structures that discourage harmful behaviors and encourage best practices, as well as mechanisms that deliver justice to affected individuals in the form of compensation for experienced harms.[18] This section will outline four challenges for litigation-based paths to accountability: lack of awareness of targeted individuals, the obscurity of spyware vendors, difficulties establishing jurisdiction, and risks of exposing technical information.

## Awareness of targeted individuals

Awareness of spyware use is an essential prerequisite to accountability. Spyware is designed to be undetectable to victims and often can only be detected with advanced forensic analysis. Without knowledge or suspicion of spyware use, individuals whose devices are compromised may be unable to pursue justice or take countermeasures to protect themselves, their contacts, or their communications. In some cases, activists, dissidents, and journalists may be aware of the cybersecurity risks they face due to the nature of their work or their identities. Individuals may be unaware of organizations and resources that could provide support, or fear repercussions for themselves and their contacts if caught contacting or engaging with advocacy organizations or other targeted individuals.

To date, policymakers have focused on responding to incidents where individuals or groups became aware of targeting, particularly when the use of a spyware capability can be attributed to specific actors or spyware vendors. For example, the Pegasus Project, an international investigative journalism initiative that drew attention to spyware vendor NSO Group's Pegasus spyware tool prompted the creation of a European Parliament committee to examine use of Pegasus and the inclusion of NSO Group on the US Department of Commerce's Entity List.[19]

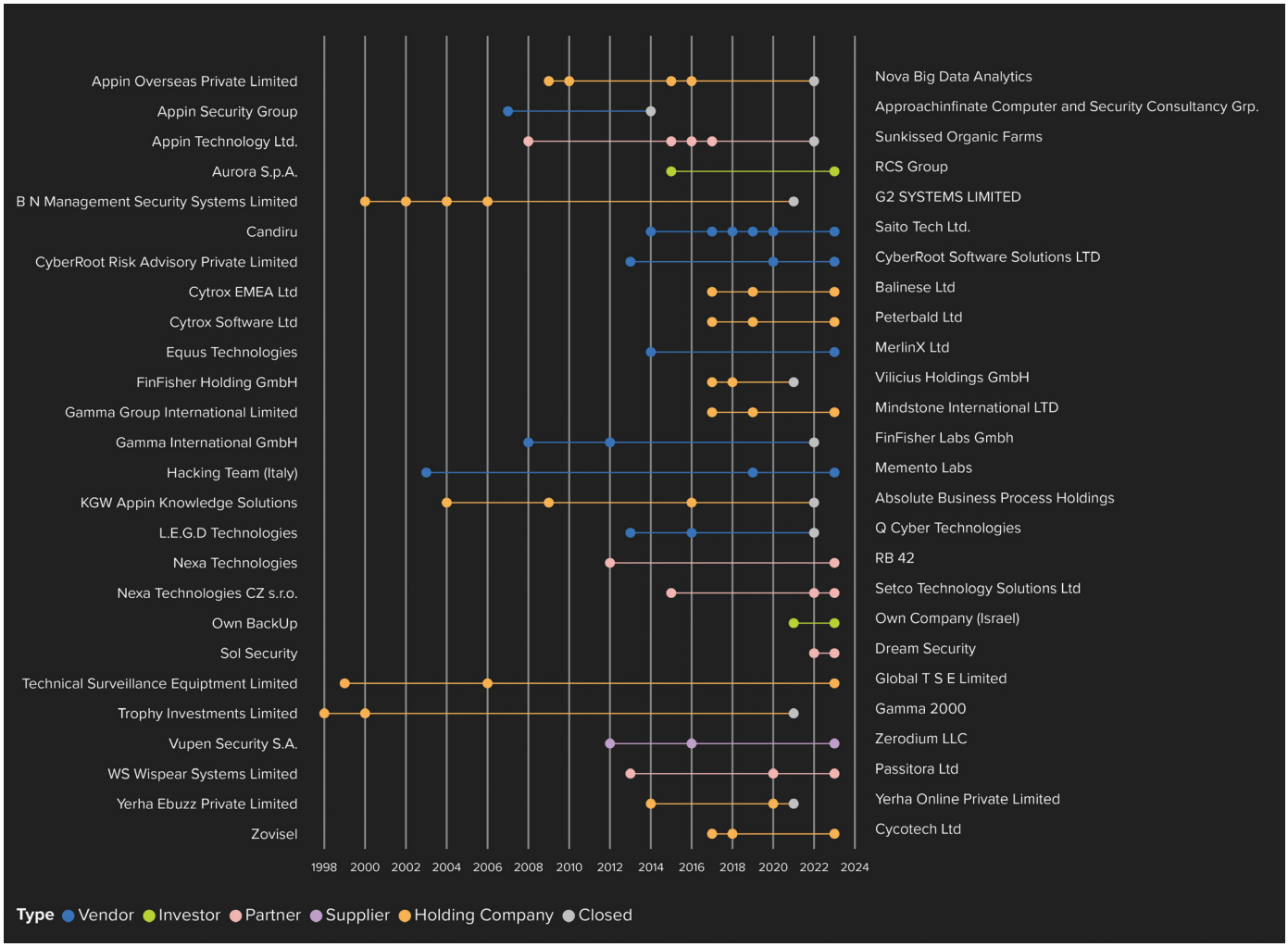
Awareness of the impacts and harms of spyware has increased over the last few years due to the important actions of civil society investigative work. In high-profile cases such as the campaign against human rights activists, journalists, and lawyers in Mexico, victims and their affected family members have collaborated with research and advocacy groups, including Citizen Lab, Amnesty International, and Access Now, to attribute suspicious text messages to attempts to install NSO Group's Pegasus on their devices.[20] In recent cases, including the use of Paragon's Graphite against European journalists and either NSO Group or Candiru's tools against prominent members of civil society in Catalonia, threat notifications from Apple and WhatsApp have prompted forensic investigations from Citizen Lab, which confirmed the presence of spyware.[21] Without suspicion and subsequent confirmation of spyware use, individuals cannot pursue legal action against spyware vendors.

## Obscurity of the spyware market

Another obstacle to accountability for spyware vendors is the obscurity of the spyware market. Prior research including the Atlantic Council's *Mythical Beasts* report, which maps the spyware ecosystem and imposes transparency on the market, outlines tactics used by spyware vendors to obfuscate their identities.[22] Without attribution of a spyware infection to a specific vendor, litigation cannot achieve accountability from specific vendors for specific harms.[23]

18. Allison Pytlak et al., *Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches, Stimson Center*, July 8, 2024. https://www.stimson.org/2024/advancing-accountability-in-cyberspace/; Freedman Consulting, *Spyware Accountability Mechanisms Framework*, *Ford Foundation and Open Society Foundations*, https://tfreedmanconsulting.com/wp-content/uploads/sites/264/Spyware-Mechanisms-Framework_Final.pdf.
19. "The Pegasus Project," Amnesty International Security Lab, accessed September 13, 2025, https://securitylab.amnesty.org/case-study-the-pegasus-project/; European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, "Spyware as a Threat to Fundamental Rights and Democracy in the EU," April 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/761472/IPOL_BRI(2024)761472_EN.pdf.
20. John Scott-Railton et al., "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," *The Citizen Lab*, June 19, 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.
21. Bill Marczak and John Scott-Railton, "Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted," *The Citizen Lab*, June 12, 2025, https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/; John Scott-Railton et al., "CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru," *The Citizen Lab*, April 18, 2022, http://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.
22. Roberts et al., *Mythical Beasts and Where to Find Them*.
23. Roberts et al., *Mythical Beasts and Where to Find Them*.

**Fig. 1:** Name changes for entities studied in the Mythical Beasts project (1992-2023).




Source: Roberts et al., Mythical Beasts and Where to Find Them.

As outlined in *Mythical Beasts*, spyware vendors often change names, in some cases multiple times, to hide their identities and potentially to mitigate the business impacts of negative reporting. For example, the vendor Candiru Ltd changed its names four times in rapid succession from 2016 to 2020 and now operates as Saito Tech Ltd.[24] Figure 1 highlights various entities within the spyware market that have changed names. Without consistent naming conventions and legal records, civil society organizations, targeted individuals, and corporations are often unable to pin down responsible entities and individuals, which enables them to act with impunity.

Spyware vendors also engage in corporate restructuring, including opening branches, procuring subsidiaries, developing strategic partnerships, or creating supplier relationships, which can make it difficult to attribute spyware incidents to specific entities.[25] In depositions from the WhatsApp case against NSO Group, an individual working for Q Cyber Technologies, part of NSO Group, noted that there was no practical difference between employees of NSO Group and Q Cyber, despite legal distinctions between the companies.[26]

Spyware vendors engage in strategic jurisdiction hopping, often in conjunction with corporate restructuring tactics, to evade accountability and allow for the promotion and sale of

24. Roberts et al., *Mythical Beasts and Where to Find Them*.
25. Roberts et al., *Mythical Beasts and Where to Find Them*.
26. *Deposition of Sarit Bizinsky Gil*, WhatsApp Inc., et al. v. NSO Group Technologies Limited, et al., No. 4:19-cv-07123-PJH (N.D. Cal.), September 6, 2024, https://about.fb.com/wp-content/uploads/2025/05/WhatsApp-v-NSO-Gil-Transcrips_Case-4-19-cv-07123-PJH.pdf.

**Fig. 2:** Entities in the Mythical Beasts dataset that cross jurisdictional boundaries).


Source: Roberts et al., Mythical Beasts and Where to Find Them.

their products in other countries, enabling them to take advantage of more permissible legal environments.[27] Figure 2 highlights the cross-jurisdictional connections present across a sample of the spyware market.

## Difficulties establishing jurisdiction

Suits against spyware vendors also face the obstacles of finding an appropriate venue. In a lawsuit against a spyware vendor, relevant physical locations can be both varied and difficult to determine. It is a considerable challenge to verify the corporate nationality or countries of activity of the spyware vendor, the location of the targeted devices, the citizenship and residence of the targeted individual, the locations of the company and computing infrastructure providing the technology product targeted by the spyware, and the legal status of the purchaser of the spyware tool. The distributed, decentralized nature of the harms in these cases can make it difficult to determine which courts are the correct avenues for claims against spyware vendors and, therefore, have jurisdiction to hear a case.

In practice, several high-profile lawsuits have not overcome the jurisdiction hurdle. The widow of assassinated *Washington Post* journalist Jamal Khashoggi's suit against NSO Group was dismissed by the US Court of Appeals for the Fourth Circuit due to a lack of personal jurisdiction over the defendant in Virginia in May 2025, despite the argument that spyware was used against the widow while she was in Virginia.[28] A case in California, brought by El Salvadoran journalists against NSO Group, was also dismissed but will be reconsidered after an

27. Roberts et al., *Mythical Beasts and Where to Find Them*.

28. Joe Dodson, "Widow of Slain Saudi Journalist Can't Pursue Surveillance Claims Against Israeli Spyware Firm," *Courthouse News Service*, May 21, 2025, https://www.courthousenews.com/widow-of-slain-saudi-journalist-cant-pursue-surveillance-claims-against-israeli-spyware-firm/.

appeals court found in July 2025 that the dismissal did not fully evaluate the relevant forum choice considerations.[29] The WhatsApp case overcame jurisdictional barriers in part because the case involved US citizens and residents, and in part because the court relied upon WhatsApp's evidence that "Pegasus code was sent through plaintiff's California-based servers forty-three times during the relevant time period."[30]

Spyware vendors have also invoked sovereign immunity as a defense, claiming that their role as agents of foreign governments shields them from legal action in US courts. The Supreme Court denied NSO Group's petition to hear their sovereign immunity defense, allowing the Ninth Circuit's decision to stand— that NSO is not entitled to sovereign immunity—in agreement with an amicus brief from the Justice and State Departments.[31] In the United Kingdom courts have gone further, determining that even foreign states are not immune from litigation and allowing cases against Saudi Arabia for the use of NSO Group's spyware and Bahrain for the use of Gamma Group's spyware.[32]

Clearing the bar of establishing jurisdiction is one obstacle that has plagued recent spyware cases in the United States. As jurisdiction must be established before a court can hear the merits of a case, lurking behind jurisdictional concerns may be a number of other legal difficulties.

## Exposure of attribution information

Another obstacle to successful litigation against spyware vendors is the risk of exposing methods of detection and other valuable research sources to spyware vendors. For the purpose of this work, it is sufficient to understand that researchers can "fingerprint" spyware based on technical traces or patterns of behavior of spyware vendors, enabling attribution of spyware infections to specific vendors or spyware tools.[33] However, public disclosure of that information can risk alerting spyware vendors to the details upon which researchers rely to detect spyware infections and infrastructure, allowing for the adoption of new tactics, and thus enabling vendors to keep their tools one step ahead of targeted individuals.[34] In September 2024, Apple dropped an ongoing lawsuit against NSO Group, citing its preference to avoid the risk of exposing threat intelligence and detection capabilities during litigation.[35] This illustrates a tradeoff between the benefits of public disclosure of indicators and the risks of alerting spyware vendors to detected techniques.[36]

Researchers and technology companies can choose to divulge details to inform and protect the public, exposing information like domain names, email addresses, and process names that spyware vendors use.[37] This disclosure often prompts spyware vendors to shift to new infrastructure configurations in order to avoid detection and attribution.[38] Maintaining the secrecy of certain technical indicators of spyware infections

29. Tim Starks, "Legal Barriers Complicate Justice for Spyware Victims," *CyberScoop*, October 30, 2024, https://cyberscoop.com/spyware-court-cases-nso-group-meta-whatsapp-apple/; Tim Starks, "Appeals Court Clears Path for El Salvadoran Journos to Sue Spyware Maker," *CyberScoop*, July 8, 2025, https://cyberscoop.com/appeals-court-clears-path-for-el-salvadoran-journos-to-sue-spyware-maker/.
30. WhatsApp Inc., et al. v. NSO Group Technologies Limited, et al., "Order Re Motions for Summary Judgment, Motion for Sanctions, and Discovery Letter Briefs," No. 19-cv-07123-PJH, U.S. District Court for the Northern District of California, filed December 20, 2024, https://storage.courtlistener.com/recap/gov.uscourts.cand.350613/gov.uscourts.cand.350613.494.0.pdf.
31. NSO Group Technologies Limited, et al. v. WhatsApp Inc., et al., No. 21-1338, Supreme Court of the United States, petition for certiorari denied January 9, 2023, https://www.supremecourt.gov/docket/docketfiles/html/public/21-1338.html; NSO Group Technologies Limited, et al. v. WhatsApp Inc., et al., "Brief for the United States as Amicus Curiae," No. 21-1338, Supreme Court of the United States, filed November 21, 2022, https://www.supremecourt.gov/DocketPDF/21/21-1338/247116/20221121154250394_NSO%20v.%20WhatsAppp%20CVSG.pdf.
32. "Court of Appeal Upholds Ruling that a Foreign State Can Be Sued for Alleged Hacking of Computers," Twenty Essex, October 7, 2024, https://www.twentyessex.com/court-of-appeal-upholds-ruling-that-a-foreign-state-can-be-sued-for-alleged-hacking-of-computers/; "High Court rules that a foreign state can be sued for alleged use of spyware," Twenty Essex, August 22, 2022, https://www.twentyessex.com/high-court-rules-that-a-foreign-state-can-be-sued-for-alleged-use-of-spyware/.
33. Bill Marczak et al., "Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains," *The Citizen Lab*, April 18, 2023, https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/.
34. Marczak et al., "Triple Threat."
35. Joseph Menn, "Apple Seeks to Drop its Lawsuit Against Israeli Spyware Giant NSO," *Washington Post*, September 13, 2024, https://www.washingtonpost.com/technology/2024/09/13/apple-lawsuit-nso-pegasus-spyware/.
36. Marczak et al., "Triple Threat."
37. Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, July 18, 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.
38. Amnesty International, *Forensic Methodology Report*.

can also enable the attribution of future attacks, as a Citizen Lab report on FORCEDENTRY indicates.[39]

Spyware vendors have proven that they can bounce back from the public exposure of their infrastructure and continue to operate, as was the case with the Intellexa Consortium. In at least three instances beginning in 2023, Intellexa Consortium's infrastructure was exposed by civil society researchers at Amnesty International, Recorded Future's Insikt Group, and Sekoia, resulting in an internal takedown of their infrastructure, which impacted the consortium's ability to deploy or maintain infections, and was compounded by US Department of Treasury sanctions on members of the Intellexa Consortium in 2024.[40] Despite these efforts by civil society, the private sector, and the US government, the Intellexa Consortium adapted and rebuilt its exposed infrastructure at an alarming speed.[41] According to Recorded Future, the Intellexa Consortium continues to operate in 2025.[42]

39. Bill Marczak et al., "FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild," *The Citizen Lab*, September 13, 2021, https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/.
40. AJ Vicens, "Predator Spyware Infrastructure Taken Down after Exposure," *CyberScoop*, March 4, 2024, https://cyberscoop.com/predator-spyware-infrastructure-taken-down/; *US Department of the Treasury,* "Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium,", press release, March 5, 2024, https://home.treasury.gov/news/press-releases/jy2155.
41. Insikt Group, *Predator Spyware Infrastructure Returns Following Exposure and Sanctions*, *Recorded Future*, September 5, 2024, https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions.
42. Insikt Group, *Predator Still Active, with New Client and Corporate Links Identified, Recorded Future*, June 12, 2025, https://www.recordedfuture.com/research/predator-still-active-new-links-identified.

# Overcoming accountability obstacles

While litigation and other accountability action that technology companies such as Apple (iMessage, iPhone), Google (Android), and Meta (WhatsApp) pursue are not immune from the aforementioned obstacles, these companies have unique capabilities with which to push back against the risks and harms of spyware and to overcome those obstacles. Technology companies' litigation and preventative action do not necessarily involve direct victim compensation or justice for previous harms, but can act as an important preventative measure for future harms of spyware, complementing other approaches to accountability. Four essential capabilities of technology companies will be discussed in this section: unmatched technical insights and awareness, preexisting user relationships, the ability to directly secure products from spyware, and the ability to offer opt-in security features.

## Technical insights and awareness

As developers, maintainers, and sellers of technology products, technology companies are best situated to identify and make sense of technical signals of spyware abuse. As the manufacturers of devices, companies like Apple shape the use of their products through both the development of operating systems and choices about third-party access to devices, including what applications are available on app stores.[43] Apple cites its closed ecosystem as a security benefit, highlighting controls that prevent developers from accessing sensitive user data without permission.[44] Advanced spyware tools, such as zero-click exploits, overcome the security controls that operating system and messaging platform developers promote.[45]

Technology companies also have visibility across campaigns through the infrastructure they operate to deliver services. According to a 2021 Apple complaint, the technology firm determined that NSO Group obtained more than one hundred Apple IDs and stored an encrypted Pegasus payload on iCloud servers as part of executing the spyware.[46] Companies whose products are not directly targeted by spyware might also have useful information and the ability to intervene, as illustrated by Amazon Web Services (AWS) shutting down NSO Group's access to the firm's cloud content delivery network (CDN) service in 2021.[47] Companies can utilize these technical insights directly, eliminating infrastructure access or as evidence in litigation against spyware vendors, or share them with members of civil society and targeted individuals who are pursuing accountability.

## Ease of notification

Technology companies with consumer-facing products already have relationships with affected victims, making the task of threat notification easier than alternative approaches. Instead of relying on emails or text messages from third-party sources, which to individuals could resemble either spam or further attempts to infect their devices with spyware, companies like Apple, Meta, and Google have multiple options to privately and proactively communicate with affected individuals in a way that is distinguishable from a third-party source. As developers, technology companies have the unique ability to push notifications directly to users via banners, settings, or account menus, or dedicated security pages within an app, operating system, or messaging platform. The reinforcement of notifications across email, text, and push notifications or via banners on user's settings pages, as well as more specialized features like security check-up pages, all allow users to distinguish threat notifications from spam or third-party harassment.

In the past, technology companies including Meta, Apple, and Google have used several of these methods to notify individuals of the likely use of spyware against their devices or communications.[48] The further use of this capability could improve

43. Apple Inc., *Building a Trusted Ecosystem for Millions of Apps: The Important Role of App Store Protections,*" white paper, June 2021, https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf.
44. Apple Inc., *Building a Trusted Ecosystem*.
45. Zack Whittaker, "Apple Patches an NSO Zero-Day Flaw Affecting All Devices," *TechCrunch*, September 13, 2021, https://techcrunch.com/2021/09/13/apple-zero-day-nso-pegasus/.
46. Apple Inc. v. NSO Group Technologies Limited, and Q Cyber Technologies Limited, "Complaint: Demand for Jury Trial," filed November 23, 2021, https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf.
47. Dan Swinhoe, "AWS Kicks NSO Group from its Infrastructure After Hacking Report," *Data Center Dynamics*, July 21, 2021, https://www.datacenterdynamics.com/en/news/aws-kicks-nso-group-from-its-infrastructure-after-hacking-report/.
48. Zack Whittaker, "Google is Notifying Android Users Targeted by Hermit Government-Grade Spyware," *TechCrunch*, June 23, 2022, https://techcrunch.com/2022/06/23/hermit-zero-day-android-spyware/; "Protecting Users from Spyware," *WhatsApp*, accessed September 15, 2025, https://faq.whatsapp.com/641700318302674; Zack Whittaker, "WhatsApp Fixes Zero-Click Bug Used to Hack Apple Users with Spyware," *TechCrunch*, August 29, 2025, https://techcrunch.com/2025/08/29/whatsapp-fixes-zero-click-bug-used-to-hack-apple-users-with-spyware/; "About Apple Threat Notifications and Protecting Against Mercenary Spyware," *Apple*, April 23, 2025, https://support.apple.com/en-us/102174.

awareness of exposure to the risks of spyware, prompting follow-on accountability actions.

## Hardening products against spyware

Technology companies can take another important step toward combatting spyware: directly securing their products. Spyware tools exploit vulnerabilities or misconfigurations in software which, while technically challenging to avoid, detect, or remedy, depend almost entirely on the development decisions and practices of technology companies. Chained-together vulnerabilities, which comprise a zero-click exploit, can only be conclusively stamped out with a patch issued by the organization responsible for the product or device. In the case of FORCEDENTRY, a NSO Group exploit targeting Apple's image library, Citizen Lab discovered an artifact on an infected phone, which the researchers then forwarded to Apple for analysis and remediation.[49] In response, Apple promptly issued a patch and notified customers via a security update.[50] In that case and several others, Apple's security team deserves praise for both their efforts to remediate the underlying vulnerability and the speed of their response. Unfortunately, if a company responsible for an operating system or messaging platform chose not to behave as Apple did in this case, targeted individuals and researchers would have minimal leverage to incentivize other behavior.

## Offering additional security features

Consumers choose the platforms, apps and operating systems they use, but with a few notable exceptions, they do not possess the ability to adjust design and root functionality of their devices to protect themselves from spyware. However, technology companies can offer opt-in security features, which may prevent the use of certain device features, but ultimately provide stronger security. Since 2022, Apple has offered Lockdown Mode, which restricts certain functionality on Apple devices in exchange for heightened protections from spyware.[51] As part of its bug bounty program, Apple has also doubled payouts to researchers identifying vulnerabilities that affect devices in Lockdown Mode.[52] Google offers a free Advanced Protection Program for Google Accounts, which requires the use of a passkey or security key, provides additional warnings for downloads, and enables other optional security settings.[53] Advocacy organizations and researchers, including Citizen Lab and Amnesty International, have endorsed these optional features. Only the companies that provide these products and services can offer hardened versions, which remain licensed versions of their offerings, highlighting the critical role these companies play in shaping the security ecosystem.

49. Marczak et al., "FORCEDENTRY."
50. Whittaker, "Apple Patches."
51. Jackie Snow, "The iPhone's Lockdown Mode: What It Is and Who Should Consider Using It," *Wall Street Journal,* November 30, 2024, https://www.wsj.com/tech/cybersecurity/iphone-lockdown-mode-e1901a85?st=ej1wAy&reflink=desktopwebshare_permalink.
52. "Apple Expands Industry-Leading Commitment to Protect Users from Highly Targeted Mercenary Spyware," *Apple,* updated July 6, 2022, https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/.
53. *Google,* "Google's Strongest Security Helps Keep Your Information Safe," accessed September 9, 2025, https://landing.google.com/intl/en_in/advancedprotection/.

# Shifting responsibility with products liability for software

Efforts to achieve spyware accountability have focused on justice delivered through the courts and litigation. An adjacent policy debate around the challenge of redistributing responsibility for software insecurity has resulted in proposals to apply the legal scheme of common law products liability to software. This section provides an overview of the legal basis for proposals aimed at shifting incentives in the private sector for software insecurity, and explores the advantages and disadvantages of such a structure for spyware accountability. The authors also offer a proposal for a legislative safe harbor structure, which if implemented, could reshape incentives for technology companies to assist in the pursuit of accountability for spyware. The structure would have several essential features, as outlined in the table below.

## Software liability 101

The core premise of software liability proposals is straightforward: the costs of software failures are poorly distributed, with customers bearing the costs of security failures while vendors face little incentive to invest in security. Advocates argue that the market for software security is misaligned, with too little cost attached to the sale of insecure software products and services, while opponents argue that the result of this proposal would be to impose too heavy of a burden on software companies.[54] However, the legal concepts underpinning these proposals are anything but straightforward and assessing such proposals can require fluency with both case law and complex legal theories. This section is not intended as a comprehensive overview of all proposals related to applying products liability to software; for a more detailed exploration of such proposals, refer to the Cyber Statecraft Initiative's *Design Questions in the Software Liability Debate* report and the Law-

**Table 1:**

| Design Question | Description | Safe Harbor Implementation |
|---|---|---|
| Applicable Harms | What harms qualify under this implementation? | Harms resulting from the infection or targeting of devices or software by spyware vendors. |
| Standards or Duties of Care | What practices must technology companies follow to benefit from this implementation? | Comprehensive threat notification and detection, information sharing, enhanced security features, rapid remediation of identified flaws. |
| Scope of Enforcement | To which kinds of software, or technology companies, does this implementation apply? | Messaging platforms, mobile operating systems, and companies responsible for those systems. |
| Governance | Which entities would determine compliance with this implementation? | At the federal level, certification of compliance with standards could be carried out by an independent regulatory agency such as the Federal Trade Commission (FTC), bifurcated from court assessment of claims to which it would apply. |

54. Maia Hamin et al., *Design Questions in the Software Liability Debate*, *Atlantic Council,* January 16, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/design-questions-in-the-software-liability-debate/.

fare Institute's series on this topic, which features research by Atlantic Council fellow Chinmayi Sharma.[55]

Products liability is a subset of tort law. For the purposes of this brief, it is sufficient to understand that litigation involving torts does not require government intervention to enforce but grants victims the right to sue and receive compensation for harms suffered.[56] Two main obstacles explain the lack of successful products liability cases against software vendors for insecure software at present. Defining software as a product, and thus eligible for a products liability framework, is difficult because software is legally treated as text or an intangible product governed by copyright and licensing regimes.[57] The economic loss rule prevents litigation for solely economic harms under tort law, which would be a barrier to any litigation that does not involve physical damage.[58] Proposals for products liability regimes designed to address insecure software often refer both to standards of care and safe harbors.[59] The critical point is that, in the context of these proposals, **standards of care define acceptable and reasonable conduct by software developers and manufacturers, while safe harbors provide protection from litigation to entities that comply with certain, specified practices**.[60]

Several legislative proposals have emerged over the last few years to create a statutory federal products liability regime for software in the United States. The Cyberspace Solarium Commission proposal for applying liability to software suggests creating a standard of care for software products that requires companies to patch vulnerabilities within ninety days of discovery or reporting.[61] Companies that fail to comply with that standard of care would be liable for economic harms greater than $75,000, physical damage, and harm to physical safety or security, with end users able to sue for damages, court costs, and attorney fees capped at 15 percent of the company's annual revenue the year prior.[62]

The Biden administration's proposal for a software liability regime emerged from its National Cybersecurity Strategy (NCS), which argued that "Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end users that often bear the consequences of insecure software." [63] The NCS proposal suggested an "adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services," involving the National Institute of Standard and Technology to inform the codification of secure software development standards.[64] A proposal from Jim Dempsey, as part of *Lawfare*'s Secure by Design paper series, suggests a three-part regime for insecure software liability.[65] The Dempsey proposal also includes a safe harbor, which would shield developers from liability if they comply with a set of best practices for software security. [66] Industry groups and trade associations, including the Business Software Alliance in its 2025 Global Software Agenda, have also argued that a safe harbor premised on secure development standards would drive more companies to adopt those standards, strengthening the security of the overall software ecosystem.[67]

## A path forward for spyware liability

The use of spyware capabilities against individual mobile devices represents an extreme form of a common security failure, which is the exploitation of insecure software by a malicious actor. In the spyware market, highly motivated and well-resourced threat actors continue to procure vulnerabilities and target individuals with sophisticated capabilities. Even the strictest secure development standards cannot eliminate all vulnerabilities, and under some proposed frameworks of lia-

55. Hamin et al., *Design Questions*; Chinmayi Sharma and Benjamin C. Zipursky, "Who's Afraid of Products Liability? Cybersecurity and the Defect Model," *Lawfare*, October 19, 2023, https://www.lawfaremedia.org/article/who-s-afraid-of-products-liability-cybersecurity-and-the-defect-model.
56. Sharma and Zipursky, "Who's Afraid of Products Liability?"
57. Sharma and Zipursky, "Who's Afraid of Products Liability?"
58. Sharma and Zipursky, "Who's Afraid of Products Liability?"
59. Derek E. Bambauer and Melanie J. Teplinsky, "Standards of Care and Safe Harbors in Software Liability: A Primer," *Lawfare*, May 31, 2024, https://www.lawfaremedia.org/article/standards-of-care-and-safe-harbors-in-software-liability--a-primer.
60. Bambauer and Teplinsky, "Standards of Care."
61. US Cyberspace Solarium Commission, "Legislative Proposals," July 2020, https://www.solarium.gov/report/legislative-proposals.
62. US Cyberspace Solarium Commission, "Legislative Proposals."
63. The White House, "National Cybersecurity Strategy," March 2023, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
64. The White House, "National Cybersecurity Strategy."
65. Jim Dempsey, "Standards for Software Liability Focus on the Product for Liability, Focus on the Process for Safe Harbor," *Lawfare,* January 23, 2024, https://www.lawfaremedia.org/article/standards-for-software-liability-focus-on-the-product-for-liability-focus-on-the-process-for-safe-harbor.
66. Dempsey, "Standards for Software Liability."
67. Business Software Alliance, "BSA's 2025 Global Agenda: The Enterprise Technology Sector's Agenda for a Secure and Resilient Digital Ecosystem," October 2024, https://www.bsa.org/files/policy-filings/2025cyberagendabsa.pdf.

bility, only unpatched vulnerabilities would enable customers to collect damages from companies. However, the spyware ecosystem has several characteristics that complicate the ability of the above proposals to resolve the harms of spyware or realign incentives in the spyware ecosystem.

As discussed previously, obstacles to spyware accountability through litigation—i.e., a lack of awareness of targeted individuals, the intentional obscurity of spyware vendors, difficulties establishing jurisdiction, and the risks of exposing research—complicate the ability of individuals affected by spyware to successfully bring lawsuits addressing the harms of spyware. Rather than expecting a general proposal for applying products liability to resolve the harms of spyware, this report proposes a targeted application of concepts from those proposals to the specifics of the spyware ecosystem. This legislative safe harbor framework could be a component of a broader policy regime designed to shift incentives and responsibility for insecure software, or function as a standalone structure designed to incentivize technology companies to pursue and support spyware accountability.

Three considerations should shape the development of a safe harbor framework, which would shield technology companies from litigation resulting from the application of products liability to software, or related litigation designed to hold software companies to account for the insecurity of their products.

1. Any policy intervention should recognize the heightened threat environment that technology companies face when defending against state-sponsored or affiliated spyware vendors.

Unlike financially motivated cybersecurity incidents, which might principally target well-resourced institutions, spyware often targets journalists, activists, dissidents, and human rights defenders, whose communications and activities are already subject to state scrutiny and repression. As discussed, technology companies possess capabilities to push back against spyware vendors. However, perfect security against well-resourced, nation-backed actors is neither technically feasible nor economically reasonable to expect from private companies that do not have total control over how users operate and use their platforms and systems. Companies can also face backlash from governments as they implement security practices that have the effect of restricting governments, particularly law enforcement agencies, from accessing information of interest or notify individuals of government use of spyware.

2. The rapidly evolving nature of both spyware capabilities and defensive technologies also requires a framework that can adjust to new threats and incorporate emerging best practices.

Adaptability should be built into the framework's structure rather than requiring legislative amendments for each technological development. Without such flexibility, especially related to the nature of information that can be shared about spyware threats, defenders could quickly find themselves out of step with effective practices for mitigating the harms of spyware. Legislation and regulatory frameworks should not be expected to fully predict the evolution and transformation of an ecosystem as complex as the spyware market, but the historical pace of change within the market suggests that policymakers should anticipate new and different threats to continue to emerge.

3. The nature of the spyware ecosystem requires careful international engagement, as the challenges of spyware are not contained within the borders of the United States.

The involvement of other countries in responding to or perpetuating spyware is a critical consideration for any domestic policy proposal, as other countries could undermine or take advantage of carelessly designed policies. For example, requiring additional reporting or notification to governments globally about the identities of spyware victims or of technical indicators of compromise of spyware could tip off spyware customers to the detection of their spyware use. Policy interventions that create additional requirements and mechanisms for governments to shape the behavior of technology companies could also be abused to compel companies and organizations responsible for the security of messaging platforms and operating systems to disclose further information about customers or end users. As international efforts continue to address the harms of spyware, including the UK and France-led Pall Mall Process, which applies diplomatic levers to constrain the growth of spyware, US engagement in international forums and collaboration with aligned governments will be essential to the effectiveness of any framework designed to deliver spyware accountability.

## A safe harbor for spyware

In response to the above considerations, this report proposes a spyware-focused safe harbor framework that would incentivize technology companies to engage in best practices for spyware accountability by shielding them from litigation related to spyware's harms. This would include any future litigation resulting from the application of a products liability standard to software insecurity. The details of the proposed safe harbor are included below and are referenced in the summary table at the beginning of this section.

1. Standards or duties of care that would make a technology company eligible for the safe harbor's shield should include **comprehensive threat notification and detection, information sharing, enhanced security features, and rapid remediation of identified flaws**.

Threat notification represents a particularly critical component of this framework. Technology companies that proactively notify users of suspected spyware targeting, provide clear guidance on protective measures, and facilitate connections with relevant support organizations should be shielded from claims related to the initial compromise, and will play a critical role in

addressing the challenges of victims' awareness of spyware infections.

Information sharing with researchers, advocacy organizations, and other technology companies is another crucial area for safe harbor protections. Companies that responsibly share threat intelligence with organizations like Citizen Lab, Amnesty International, and other established research entities should receive liability protections, provided they follow established guidelines for protecting sensitive information and user privacy. This sharing is vital to addressing the challenges presented at the start of the paper, including aiding with visibility of spyware incidents, including enabling investigative research by civil society organizations, and decreasing the obscurity of the spyware market, while respecting companies' legitimate concerns with exposing sensitive security information to the public.

The framework should also reward companies that offer opt-in enhanced security features, such as Apple's Lockdown Mode or Google's Advanced Protection Program. These features require significant development effort and financial resources, including when tied to bug bounty programs. By providing safe harbor protections for companies that invest in developing and maintaining these specialized security offerings, the framework would encourage broader adoption of such protective measures across the industry.

Finally, rapid remediation of vulnerabilities or exploit chains is a step that only technology companies can take to respond to ongoing spyware campaigns. By patching devices and updating messaging platforms, technology companies curb infections and protect users from harm. While developing patches and mitigating flaws should not be rushed—as developers and technology companies must completely evaluate software changes to ensure they completely fix flaws without disrupting functionality—companies should be rewarded for the rapid mobilization of effort that quick patching requires.

2. Eligible harms should include **harms resulting from the infection or targeting of devices or software by spyware vendors**.

Harms that would trigger application of the safe harbor shield should be limited to those caused by spyware capabilities. Qualifying incidents would involve targeted capabilities, such as the use of zero-day exploits and individual persistent device access, but not general cybersecurity incidents, which are shaped by a wide variety of incentives. As the discussion of applying products liability to software broadly indicates, a host of legal barriers and considerations would shape the implementation of such a regime. To minimize disruption to broader cybersecurity incentives, this safe harbor shield should apply narrowly to harms specific to the spyware ecosystem. However, this would not make this proposal's tailored proposal incompatible with a broader software liability structure based on products liability, and the implementation of such a safe harbor would not require policymakers to intervene in or decide other debates related to those proposals and broader software security challenges.

3. Eligible technologies and products should include **messaging platforms, mobile operating systems, and the companies responsible for the security of those systems** or involved in their development and operation.

The safe harbor should apply to technology sectors that are targets of sophisticated spyware tools, particularly messaging platforms like WhatsApp and iMessage, as well as mobile operating systems including iOS and Android. Companies eligible for protection should include primary developers and operators of these platforms, plus entities involved in their security infrastructure such as cloud service providers hosting messaging services or companies providing security services. This scope recognizes that spyware campaigns often exploit vulnerabilities across interconnected systems and that effective defense requires coordination among stakeholders.

4. **Compliance with standards should be determined by a government entity outside of the judicial system**, which would certify compliance to court entities for the purposes of litigation.

Certification of compliance with standards could be carried out by an independent regulatory agency, such as the FTC, but would occur separately from judicial assessment and adjudication of claims where the safe harbor would be relevant, maintaining important neutrality from policy departments and the legal system while still providing a critical verification role. This would prevent judicial bodies from having to make esoteric technical decisions, while allowing industry and advocacy organizations to offer expertise to guide the definitions and development of best practice standards. The certification of compliance occurring outside of the judicial system could enable such standards to evolve on a regular basis, which would ensure that practices are kept up to date instead of emerging fitfully through a patchwork of case law.

At the federal level, such a framework would require careful coordination across the public and private sector, along with the participation of agencies such as the Cybersecurity and Infrastructure Security Agency, which could act as a host body to advise on the technical standards that companies would need to meet. Implementation of such a framework would require extensive consultation and testing to define effective standards for threat notification programs, information sharing protocols, and enhanced security measures. The cybersecurity community, advocacy organizations, targeted individuals, and technology companies must collaborate to ensure that any resulting standards meaningfully support accountability efforts while remaining technically feasible and economically sustainable.

# Conclusion

Spyware and the spyware ecosystem pose significant challenges that will not be resolved with any single policy intervention. The current lack of comprehensive justice or deterrence from litigation-based approaches demonstrates the need for a complementary strategy that leverages the abilities of technology companies to protect individuals from spyware while also supporting other efforts to pursue accountability.

The safe harbor framework proposed in this report offers a targeted approach to realigning incentives within the technology ecosystem. Rather than expecting general products liability proposals to address the specific challenges of spyware abuse, this framework recognizes the distinct characteristics of state-sponsored surveillance tools and the specialized role of technology companies in defending against them. By rewarding companies that invest in threat detection, user notification, information sharing, and enhanced security features, the framework could drive industry-wide improvements in protection for the journalists, activists, and human rights defenders most vulnerable to spyware targeting.

The framework's success would also depend on careful international coordination. As spyware vendors and their customers operate across jurisdictions, domestic policy interventions risk being undermined by international actors or creating opportunities for abuse by governments seeking additional leverage over technology companies. US engagement in multilateral efforts like the UK and France-led Pall Mall process will be essential to ensuring that accountability measures reinforce rather than conflict with international coordination efforts. US government support of a safe harbor proposal would demonstrate a renewed commitment to constraining spyware's harms. Such a commitment would give the United States more leverage with which to push back on countries that attempt to limit the ability of technology companies to respond to spyware's threats and engage in spyware-related abuses, ultimately preserving the ability of American technology companies to defend mobile communications and devices from national security threats.

The proposed safe harbor represents a complementary approach that acknowledges the limitations of existing accountability mechanisms while taking advantage of the demonstrated effectiveness of technology company interventions in recent spyware incidents. Developing and implementing this framework will take time, resources, and sustained commitment from policymakers, industry, and civil society. This is especially relevant in a current political climate where public-private collaboration is headed in the direction of minimizing the compliance burden upon industry, while also pushing companies to secure their products and infrastructure from the outset.

However, given the persistent threat that spyware poses to vulnerable individuals worldwide and the demonstrated inadequacy of existing accountability mechanisms, targeted policy interventions that strengthen the incentives for protective behaviors represent a critical component of a comprehensive accountability strategy. These interventions could be a useful test case for effective public-private collaboration designed to induce companies to take greater responsibility for helping to secure users over the long term. As part of broader international coordination efforts to address spyware proliferation and abuse, a well-designed safe harbor framework could provide meaningful protection for those most at risk while advancing the broader goal of accountability within the spyware ecosystem.

# About the authors

**Sara Ann Brackett** is an assistant director with the Cyber Statecraft Initiative, part of the Atlantic Council Tech Programs. She focuses her work on open-source software security, software bills of materials, software liability, and software supply-chain risk management within the Cyber Statecraft Initiative's cybersecurity and policy portfolio. Brackett graduated from Duke University, where she majored in computer science and public policy and wrote a thesis on the effects of market concentration on cybersecurity. She participated in the Duke Tech Policy Lab's Platform Accountability Project and worked with the Duke Cybersecurity Leadership Program as part of Professor David Hoffman's research team.

**Jen Roberts** is an associate director with the Cyber Statecraft Initiative, part of the Atlantic Council Tech Programs. She primarily works on CSI's Proliferation of Offensive Cyber Capabilities work. Roberts also helps support the Cyber 9/12 Strategy Challenge and is passionate about how the United States with its allies and partners, especially in the Indo-Pacific, can cooperate in the cyber domain. Roberts holds an MA in International Relations and Economics from Johns Hopkins University's School of Advanced International Studies (SAIS) where she concentrated in Strategic Studies. She also attained her BA in International Studies from American University's School of International Service.

# Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org