Atlantic Council

SPYWARE BLASTS:

Strict liability for abnormally dangerous activities

SEPTEMBER 2025

Lisandra Novo

The Atlantic Council's Strategic Litigation Project (SLP) works on legal initiatives to seek accountability for victims and survivors of human rights violations and international crimes.

Author

Lisandra Novo

Please direct inquiries to:

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

2025

Table of contents

Bottom lines up front

Journalists, members of civil society, human rights defenders, and others who have been targeted with spyware face numerous obstacles in holding those responsible accountable for abuses.

Efforts to enact binding regulation are slow and only apply to future behavior, leaving an accountability gap for past and ongoing abuses that litigation may help fill.

This report explores one theory of civil liability that has yet to be tested in spyware cases: strict liability for abnormally dangerous activities.

Executive summary

More than twenty countries have signed on to the nonbinding Pall Mall Process Code of Practice for States since it was launched in April 2025 by the United Kingdom (UK) and France.[1] Its focus is to "tackle the challenges posed by the proliferation and irresponsible use of commercial cyber intrusion capabilities (CCICs)."[2] CCICs encompass a broad array of tools, including spyware—a kind of malicious software that allows "unauthorized remote access to an internet-enabled target device" for surveillance and/or data extraction.[3] One of the pillars of the Code of Practice for States is accountability, under which countries are encouraged to establish or apply national frameworks to regulate the "development, facilitation, purchase, transfer, and use of" spyware.[4]

Establishing new domestic frameworks or even analyzing which existing national or international frameworks apply to spyware-related activity will take significant time, likely years. Meanwhile, new instances of spyware abuses against journalists and other human rights defenders continue.[5] It is therefore not surprising that the Code of Practice for States also recommends measures to incentivize responsible activity, encourage the use of export control and licensing frameworks, and provide support for victims.[6] It is on one such measure for victim support that this report focuses: "procedures for those claiming redress as a result of the irresponsible use of CCICs, including ensuring access to effective judicial or non-judicial remedies."[7] Specifically, this report explores how existing tort law relating to abnormally dangerous activities in the United States and the UK could provide a ground for bringing cases related to spyware abuses.

Tort law allows individuals to take accountability into their own hands, which is especially important when processes to enact binding obligations on actors involved in developing and selling spyware can take years and there is no guarantee they will be successful. However, tort law differs by country and, within the United States, even by state. This makes research difficult and, at a larger scale, inconsistent. Additionally, litigation is very resource intensive both in terms of money and time and governments are typically shielded from civil liability. It is simply not possible for every victim of a spyware abuse to bring a case against the actor(s) responsible. In that sense, it is not recommended to rely exclusively on tort law for accountability, but to use it as a supplementary measure while continuing to pursue parallel efforts at regulation.

With that framing, this report looks at the possibility of bringing cases under strict liability for abnormally dangerous activities in California and the UK. These two jurisdictions were chosen be-

1. Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States*, April 25, 2025, https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states.
2. Ibid.
3. 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/#about.
4. Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States*.
5. See, e.g., Lorenzo Franceschi-Bicchierai, "Researchers Confirm Two Journalists Were Hacked with Paragon Spyware," *Tech Crunch*, June 12, 2025, https://techcrunch.com/2025/06/12/researchers-confirm-two-journalists-were-hacked-with-paragon-spyware/; Kate O'Flaherty, "Apple Issues New Spyware Attack Warning to iPhone Users," *Forbes*, May 1, 2025, https://www.forbes.com/sites/kateoflahertyuk/2025/05/01/apple-issues-new-spyware-attack-warning-to-iphone-users/; "Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists," Amnesty International, press release, December 16, 2024, https://securitylab.amnesty.org/latest/2024/12/serbia-a-digital-prison-spyware-and-cellebrite-used-on-journalists-and-activists/.
6. Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States*.
7. Ibid.

cause of the similarities in their legal systems, the fact that civil cases have been brought in California against spyware developers, and since the UK is one of the countries that launched the Pall Mall Process. The author is not aware of any previous cases brought under this theory of liability with respect to spyware. Given the six-factor definition of abnormally dangerous activities in California, the fact that a court decides whether an activity qualifies, and recent developments regarding jurisdiction over foreign defendants and significant damages awards, it could be possible, although still difficult, to bring a case there under this theory related to spyware harms. The development of the same doctrine in the UK, however, cautions against attempting this novel argument there. For UK plaintiffs, more research is needed on alternative grounds under tort.

Recommendations

From these findings, several recommendations to different stakeholders can be distilled.

Targeted individuals:

- Seek digital security and advocacy support from credible organizations (like Access Now).
- Think carefully about costs, toll on mental health, risks to safety and security, and other risks posed by engaging in litigation. Consult a qualified legal representative about all these aspects.

Lawyers:

- Provide pro bono research and representation to targeted individuals.
- Collaborate with lawyers in other jurisdictions to address the transnational nature of harms.
- Collaborate with researchers and civil society groups investigating and engaging in advocacy around the misuse of spyware to better understand the complexities, risks, and other aspects of litigation.

Civil society, academia, research institutes:

- Carry out scoping research on different jurisdictions, legal and policy measures, and investigative techniques, among other topics, to advance the knowledge base and reduce the burden on legal teams and victims.

Donors:

- Provide funds for scoping research on possible grounds for investigations and cases.
- Provide adequate, multiyear financial support for litigation likely to involve substantial costs and take years; provide support for defending against Strategic Lawsuits against Public Participation (SLAPPs).
- Provide funds for technical forensic analysis.
- Provide convening spaces for civil society and experts working on spyware accountability.

Policymakers:

- Do not preempt lawsuits through regulation.
- Do not shield spyware developers or other actors involved in abuses from liability.
- Enact anti-SLAPP legislation to protect victims, researchers, and civil society advocates from retaliation.
- Continue multilateral efforts to enact binding regulation, advance norms, and pursue various accountability measures.

Introduction: Why tort law?

For example, the point that it would be "unwise" to completely rely on AI companies to self-regulate and forego other methods of controlling their behavior is especially poignant in the case of the commercial spyware industry.[8] Spyware abuses have been extensively documented by journalists and civil society.[9] Governments have publicly demanded accountability and are working toward binding obligations through the United Nations and multilateral efforts like the Pall Mall Process.[10] As experts have pointed out regarding AI, regulation is controversial and difficult to design effectively.[11] Additionally, international processes take years and regulation has its limits, so tort law can fill part of the gap.[12] Even more importantly, civil liability could be "less vulnerable to industry capture than regulation," even with resource imbalances between powerful companies and individuals.[13]

Of course, there are drawbacks to civil cases. Differences across jurisdictions reveal an "inconsistent patchwork";[14]—reliance on juries' interpretations of the law makes it difficult to predict the outcome of any given case;[15] and these cases will require technical expertise to prove cause and responsibility, something not all judges and juries may be well prepared to handle.[16] Additionally, not all actors responsible for causing AI- or spyware-related harms can be held liable in civil courts. Governments, specifically, generally enjoy immunity before foreign civil courts.[17] Lastly, civil cases themselves take many years and such delay may not result in incentives that change behavior.[18] The *WhatsApp v. NSO Group* case, for example, was originally brought in October 2019 and reached a jury verdict in May 2025, almost six years later.[19]

There is no doubt that civil litigation takes time and resources. But as national and international efforts to design and implement regulation of spyware continue, which will apply only to future conduct and violations, it is important to take advantage of accountability measures available now. Despite the near six-year journey, the jury in the *WhatsApp v. NSO Group* case did award over $167,000000 in punitive damages and over $400,000 in compensatory damages.[20] While NSO did appeal this award, which adds time and uncertainty to the case, the award is nevertheless significant.[21] Litigation should not replace regulatory or other accountability efforts but should be pursued in parallel to fill existing impunity gaps. With that framing, this report explores one theory of liability that has yet to be tested in spyware cases: strict liability for abnormally dangerous activities.

8. van der Merwe et al., "Tort Law and Frontier AI Governance."
9. See, e.g., "About the Pegasus Project," Forbidden Stories, July 18, 2021, https://forbiddenstories.org/about-the-pegasus-project/; "The Predator Files: Caught in the Net," Amnesty International, October 9, 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/.
10. Foreign, Commonwealth & Development Office, *The Pall Mall Process Code of Practice for States*; United Nations General Assembly, "Draft Final Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025," A/AC.292/2025/CRP.1, July 11, 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf.
11. van der Merwe et al., "Tort Law and Frontier AI Governance."
12. Ibid.
13. Ibid.
14. United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, "Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach," April 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf, 6.
15. Ramakrishnan et al., *U.S. Tort Liability for Large-Scale Artificial Intelligence Damages: A Primer for Developers and Policymakers*, 8.
16. van der Merwe et al., "Tort Law and Frontier AI Governance."
17. Weil, "The Limits of Liability."
18. van der Merwe et al., "Tort Law and Frontier AI Governance."
19. Lorenzo Franceschi-Bicchierai, "Eight Things We Learned from WhatsApp vs. NSO Group Spyware Lawsuit," *Tech Crunch*, May 30, 2025, https://techcrunch.com/2025/05/30/eight-things-we-learned-from-whatsapp-vs-nso-group-spyware-lawsuit/.
20. Lorenzo Franceschi-Bicchierai, "NSO Group Must Pay More than $167 Million in Damages to WhatsApp for Spyware Campaign," *Tech Crunch*, May 6, 2025, https://techcrunch.com/2025/05/06/nso-group-must-pay-more-than-167-million-in-damages-to-whatsapp-for-spyware-campaign/.
21. Suzanne Smalley, "NSO Appeals WhatsApp Decision, Says It Can't Pay $168 Million in 'Unlawful' Damages," *Recorded Future News*, June 2, 2025, https://therecord.media/nso-group-appeals-jury-award-168million-; Raphael Satter, "Court Clash between Meta and NSO Ends in $168 Million Defeat for Spyware Firm," *Reuters*, May 6, 2025, https://www.reuters.com/sustainability/society-equity/court-clash-between-meta-nso-ends-168-million-defeat-spyware-firm-2025-05-06/.

Methodology

The author of this report engaged in desk research. She consulted materials like legal opinions, legal analyses, academic articles, news reports, and outputs from civil society organizations. She consulted practitioners and received pro bono research assistance on legal questions specific to California and the UK. The author selected the United States and the UK as the jurisdictions for this report due to their governments' track records in taking active measures or calling for accountability for spyware abuses. Because tort law in the United States varies by state, a further selection needed to be made as a fifty-state survey is beyond the scope of this project. California was selected as several spyware-related civil cases have already been filed there and it is the principal place of business for a number of technology companies that sell products often exploited by spyware companies.

The Whatsapp app logo can be seen on the display of a smartphone on September 2, 2025. WhatsApp is an instant messaging service that was founded in 2009 and has been part of Meta Platforms since 2014. REUTERS/Matthias Balk

Scenario

The objective of this report is to show how the concept of liability for abnormally dangerous activities could apply to the development, sale, and use of spyware. To make this content as widely accessible as possible, the report presents a fictional fact pattern and subsequently explores how the law could apply in such a case.

Fictional fact pattern

Disclaimer: While inspired by real events, all the characters, organizations, and incidents portrayed in this section are entirely fictional and solely for illustrative purposes.

Characters:

- **Olympus Technologies:** A spyware company based in Israel that produced the spyware Delphi. Olympus Technologies maintains that it only sells to governments for law enforcement purposes and that it does not work with governments that have poor human rights records.
- **Marie:** An investigative journalist working for *Journalists FR* (*JFR*), an international newspaper based in France.
- **Pablo:** A US citizen, residing in California, and correspondent for *JFR* in the United States.
- **Iris:** A human rights advocate and barrister working for Justice Unlimited, a UK-based human rights organization.
- **Law & Legal, LLP:** A US-based firm specializing in plaintiff-side civil law claims with offices in the UK.

Incident: An unknown government agency contracts Olympus Technologies to conduct surveillance using Delphi on certain targets it claims are involved in illegal activity. While not confirmed, it is suspected that Olympus Technologies collaborates closely with governments that hire it, providing advice and support (e.g., selecting the appropriate exploit based on the intended target's behavior and devices).

Marie and Pablo suspect they were targeted by spyware due to their investigative work on human rights abuses and government corruption in several countries. Given the increase in spyware use against journalists, they contact an independent forensic expert who has previously worked with other jour-

Detailed image of a cracked smartphone screen. REUTERS/Filippo Carlot

nalists and human rights defenders. This forensic expert examines their phones and laptops and finds that their devices were infected with Delphi numerous times over a six-month period. It is not clear which government targeted them.

Marie and Pablo realize their sources and confidential information have been compromised. These sources stop collaborating with Marie and Pablo, fearing for their own and their families' safety. Marie and Pablo then approach Iris, a barrister at Justice Unlimited in the UK, for assistance. Shortly after, Iris discovers that she too has been targeted by Delphi after working with Pablo and Marie. Delphi exposes her communications with Marie and Pablo and with other human rights defenders across the world. After being notified by Iris, these contacts, also fearing for their safety, tell Iris they are concerned about their joint projects with Justice Unlimited, many years in development and some of which involve privileged and confidential legal materials.

Iris, Pablo, and Marie purchase new devices and change their contact information. Marie and Pablo ask Iris to get legal advice on how to proceed, hoping to engage in litigation or criminal investigation in at least one of the countries in which they reside.

Seeing the lawyers

Iris reaches out to Law & Legal, LLP, a US firm with offices in the UK that she has worked with before. They tell Pablo, Iris, and Marie they can explore civil claims in the United States and the UK. However, they are not familiar with French national law or European Union law and so advise them to seek local counsel there. Additionally, they cannot provide advice on criminal cases. Sophia and Winston, lawyers in California and London, first explain that their firm will take this case on pro bono, for free, but if the court allows, they will try to recover attorney fees. Theirs is a midsize firm that can afford to offer services for free to certain clients but cannot absorb all the costs of multiyear litigation. Through this structure, if possible, they could recover some reasonable costs if they win. The lawyers also encourage Pablo, Iris, and Marie to see if their contacts in civil society organizations or other larger firms would be willing to join the case as co-counsel.

The lawyers emphasize there is no guarantee any case against Olympus Technologies will be successful. A case could be dismissed at the jurisdictional phase and never reach the merits stage where the actual conduct is judged. Even if a case does make it to the merits stage, it could take years and go through numerous appeals. There is also no guarantee that a judge or jury would rule in their favor. Proceeding with a case would require a lot of time and energy from Pablo, Iris, and Marie. They may have to testify or appear for depositions. They will have to find and provide evidence to support their case. They will need to convince experts to testify or produce documentation. They may be forced to share their devices and other sensitive information for examination. Information regarding their contacts, colleagues, or family members may be revealed in discovery.

The California state flag flies above palm trees. Unsplash

Outside the courtroom, there is likely to be significant media attention, which may draw scrutiny on their personal lives, including accusations of being criminals or terrorists. Further, there are additional risks that they, their families, and the legal team could be targeted with spyware again. This can significantly interfere with someone's ability to work and spend time with family, and can have severe negative impacts on mental health. The lawyers encourage Pablo, Iris, and Marie to think carefully about the risks to themselves, their families, their colleagues, and other vulnerable contacts before deciding to pursue litigation.

Iris is already familiar with all these risks and discusses them with Pablo and Marie. They decide it is worth it to pursue a case. Sophia and Winston then have several meetings to discuss options. Civil claims can be filed under many grounds, but tort law could cover what happened to them. A tort is either an action or an omission that results in harm to a person or to property.[22] Tort law is different in the United States (where Pablo lives) and the UK (where Iris lives), and in the United States it

22. "Introduction to Tort Law," Congressional Research Service, May 26, 2023, https://www.congress.gov/crs-product/IF11291.

differs by state.[23] Within tort, there is an option that has yet to be tested in spyware cases: strict liability for abnormally dangerous activities (sometimes referred to as ultrahazardous activities). It exists both in the United States and the UK but has developed differently in these countries.

California

Why strict liability?

Sophia explains that while there are certainly difficulties in presenting a novel application like this for spyware harms, strict liability has significant benefits compared with negligence-based torts. For strict liability, there is no need to prove that a duty has been owed or breached or that the defendant had any intent to cause harm.[24] Essentially, plaintiffs need to prove only that a defendant carried out an abnormally dangerous activity, that the plaintiff has been harmed, that the harm was the kind of harm that is a foreseeable consequence of the activity, and that the defendant's carrying out of the activity was a substantial factor in causing the harm.[25] Further, there is no predetermined approved list of abnormally dangerous activities; courts decide on a case-by-case basis, which allows for more flexibility.[26]

What is the test for abnormally dangerous activities?

Sophia explains to Iris, Marie, and Pablo that strict liability for abnormally dangerous activities in California means that if a person or entity engages in an activity that is considered especially dangerous, they will be liable for harm occurring to a person, land, or property caused by such activity. This recognizes that some activities are so inherently dangerous to others that even when taking the utmost care and reasonable precautions, the risk from these activities cannot be eliminated.[27] Courts in California have a six-factor test to determine when an activity is abnormally dangerous: 1) whether there is a significant risk of harm to person, land, or chattel (property that is not land); 2) there is a chance that great harm could result from this risk; 3) the risk cannot be eliminated by exercising reasonable care; 4) whether the activity is one of common usage; 5) whether it was appropriate to carry out that activity in the place it was carried out; and 6) whether the societal value to carrying out this activity is outweighed by its risks.[28]

Typically, these cases have focused on physical or property harms from activities like handling and transporting explosives, fumigating, testing rocket motors, drilling for oil, and using open flame equipment near combustible materials.[29] These examples are clearly very different from spyware. It would be a highly novel approach to argue spyware is an abnormally dangerous activity and there is no guarantee of success. In a recent case in New York, which serves only as an example in California courts and is not binding, a court using the same six-factor test ruled that a lab's research on viruses in China could not be classified as an abnormally dangerous activity because while the virus they were studying was itself very dangerous, it was possible for the researchers to take reasonable care to mitigate the risks associated with their investigation.[30]

For any novel application, whether the doctrine would apply is a fact-specific question. But, while it may be unlikely and other attempts to expand the doctrine like that in New York have failed, it is not impossible. The main question that the court would have to decide is whether the risk inherent in spyware development and use is so unusual and impervious to mitigation measures that it would justify imposing strict liability on harms resulting from it even if carried out with reasonable care.[31]

Spyware versus typical abnormally dangerous activities

Sophia highlights that blasting with explosives, often described as the classic abnormally dangerous activity, has parallels to spyware use. First, the defendant engages in the activity for their own benefit and "is almost certainly aware of the dangers associated with" the activity.[32] Olympus Technologies develops and sells spyware to governments for profit. Numerous rights organizations and journalists have revealed lucrative contracts between the company and its government clients in the millions of dollars. These investigations also revealed many cases where these governments used Delphi to target journalists, environmental activists, members of the political opposition,

23. Ibid.
24. American Law Institute, "Strict Liability," in *Restatement of the Law Third, Torts: Liability for Physical and Emotional Harm* (American Law Institute Publishers, 2010), vol. 1, §§ 1–36, 228-29.
25. Judicial Council of California Civil Jury Instructions (2025), CACI No. 460 ("Strict Liability for Ultrahazardous Activities—Essential Factual Elements"), 371.
26. Luthringer v. Moore, 31 Cal. 2d 489, 496 (1948).
27. Jasso v. Citizens Telecomms. Co. of Cal., Inc., No. S-05-2649, 2007 U.S. Dist. LEXIS 54866, at * 10–11 (E.D. Cal. July 30, 2007); Pierce v. Pac. Gas & Elect. Co., 166 Cal. App. 3d 68, 85 (1985).
28. Jasso, 2007 U.S. Dist. LEXIS 54866, at *10–11.
29. See Green v. Gen. Petroleum Corp., 205 Cal. 328, 333–34 (1928); Luthringer, 31 Cal. 2d at 500; Smith v. Lockheed Propulsion Co., 247 Cal. App. 2d 774 (1967); Balding v. D.B. Stutsman, Inc., 246 Cal. App. 2d 559, 564 (Ct. App. 1966); McKenna v. Pac. Elec. Ry. Co., 104 Cal. App. 538, 542–43 (1930); Garcia v. Estate of Norton, 183 Cal. App. 3d 413 (1986).
30. Matter of Jones v. New York City Tr. Auth., No. 034252, 2023 N.Y. Misc. LEXIS 51267, (N.Y. Sup. Ct. Sept. 14, 2023).
31. Gjovik v. Apple Inc., No. 23-cv-04597, 2024 U.S. Dist. LEXIS 90231, at *48 (N.D. Cal. May 20, 2024).
32. American Law Institute, "Strict Liability," 233.

Dynamite explosions blast rock mass at a phosphate mine in Mdhilla, Tunisia, February 15, 2019. REUTERS/Zoubeir Souissi

and human rights defenders. The targeting was either justified on overly vague security grounds with no specific illegal conduct cited or simply not justified at all. Other spyware companies even terminated similar contracts with governments after investigations showed other instances of this, demonstrating that there is wide awareness in the sector of how some governments, democracies and autocracies alike, use (and abuse) this technology.

Second, an activity like blasting "is likely to cause harm … even though the defendant adopts all reasonable precautions in the course of conducting the … activity."[33] That is because "even when all reasonable care is exercised," blasting is still dangerous, making it "an activity whose dangerousness is 'inevitable' or 'inherent.'"[34] There are important technical and operative questions about what kind of mitigation measures, if any, a spyware company could take to prevent abuses of its technology in its contractual relationships to governments. At least for the time being, one can reasonably infer that preemptive measures to mitigate the risk of harm are either not available or not feasible from a business perspective given that other similarly situated companies have cancelled contracts in response to abuses, a measure that happens only after the harm is caused. Additionally, given the extent of investigations into abuses of this technology by governments and with new instances being reported so frequently, there is an argument to be made after so much evidence that targeting individuals beyond legitimate law enforcement purposes is not a bug but a feature of the technology as currently developed and sold.

Last, a "special feature that distinguishes blasting" is that it "causes harm essentially on its own, without meaningful contribution from the conduct of the victim or of any other actors."[35] In the classic blasting scenario, the injured victim "is a passive, uninvolved third party" who simply owns property nearby or is walking by when injured.[36] The passivity of the victims in the case of spyware abuses is beyond dispute, especially individuals who are targeted merely for being related to or otherwise in contact with the primary targets or whose private information is exposed as a result of someone else being targeted. Delphi uses a zero-click approach, meaning the person targeted literally does nothing and their device is still infected (they do not need to click on a link or visit a suspicious website, for example). Iris, Marie, and Pablo simply did their jobs and went about their lives as normal. Additionally, private conversations with and information about their contacts and

33. Ibid.

34. Ibid, 233-34.

35. American Law Institute, "Strict Liability," 234.

36. Ibid.

The logo of Israeli cyber firm NSO Group is seen on a building wall as a pedestrian passes by. REUTERS/Amir Cohen

colleagues were exposed as they had been held on Iris, Marie, and Pablo's devices.

The more difficult part to establish is whether the harms are inherent to the normal use of the spyware technology, or if governments, a third actor, are responsible for improper uses. For example, in cases relating to guns, courts in the United States have held that the possession of a dangerous instrument does not "create automatic liability when a third party takes that instrumentality and uses it in an illegal act."[37] Sophia explained that gun cases are different because US law grants immunity to gun manufacturers, and even then, there is an exception to that immunity for aiding and abetting illegal activity.[38] Spyware developers do not enjoy such immunity in the United States in the first place, so this obstacle would not apply. Further, there is credible evidence that Olympus Technologies is not completely removed from its government clients' activity after it licenses Delphi. Instead, it chooses exploits based on the government's targets and provides active technical support and assistance in the targeting at the direction of the government clients.

Who can be sued and on what basis?

Even if spyware can be classified as an abnormally dangerous activity, there are other requirements that must be met to bring a case. Only certain kinds of harms give grounds to sue—a plaintiff must show the harm is of a legally protected interest. The model California jury question sheet for ultrahazardous activities covers past and future economic losses for categories like lost earnings, lost profits, medical expenses, and similar monetary losses.[39] It also covers noneconomic losses like physical pain and/or mental suffering.[40] For Pablo, Marie, and Iris, this could mean costs incurred for replacing their devices, costs incurred for therapy and other medical expenses, unpaid time off work, and expected similar future costs. For example,

37. Bridges v. Parrish, 742 S.E.2d 794, 798 (N.C. Ct. App. 2013).

38. See León Castellanos-Jankiewicz, "SCOTUS Rules for Gun Manufacturers in Mexico Suit but Denies Blanket Immunity," *Just Security*, June 23, 2025, https://www.justsecurity.org/114981/scotus-gun-manufacturers-mexico/.

39. Judicial Council of California Civil Jury Instructions (2025), VF-407 ("Strict Liability—Ultrahazardous Activities"), 420-21.

40. Ibid.

some journalists lose their jobs as a result of loss of trust from sources. Other victims experience being shut out or ignored by friends and family who are afraid to talk to them after finding out they are under surveillance.

Further, a person or entity that engages in an abnormally dangerous activity will be held liable to anyone injured only as a proximate result of the activity, regardless of what precautions or measures are taken to mitigate the risk.[41] This is what is known as causation. Proximate cause, as defined in the California civil jury instructions for strict liability for ultrahazardous activities, requires that the harm the plaintiff suffered "was the kind of harm that would be anticipated as a result of the risk created" by the activity in question and that the defendant's carrying out of the specific activity "was a substantial factor in causing" plaintiff's harm.[42] Essentially, the reason the harm occurred has to be foreseeable and has to play a significant role in causing the harm. For spyware, having your lunch companion's wallet stolen at a restaurant near your lawyer's office would not be covered. The lunch companion is not someone whose device was targeted, plus the choice of restaurant and presence of a thief are too far removed in the causal chain and not the kind of harm that can reasonably be expected from spyware targeting.

Who can bring a case in California?

Iris, Marie, and Pablo express concern that all of them live in different countries and that Olympus Technologies is headquartered in another country. Sophia acknowledges that establishing jurisdiction over a defendant that is not in California is complicated—they must show that California out-of-state jurisdiction can apply to the defendant and that this is consistent with due process, that is, that the defendant has "minimum contacts" with the state.[43] One way to show minimum contacts is to prove the defendant is "at home" in the state, meaning a corporation's principal place of business is there, for example.[44] That is not the case for Olympus Technologies. It has no offices or personnel in California, or even the United States, and does not conduct business or ever travel there.

However, it might be possible under specific jurisdiction if the defendant has directed activities at residents there, if the case relates to activities in the state, and if exercising personal jurisdiction would be reasonable.[45] Because Pablo lives in California, his device was targeted while physically located in California, and there is the possibility that the targeting used exploits in products produced by companies that have servers in California. While this does not cover Marie and Iris, because they were targeted at the same time, likely for working together, it is possible to join their cases. There is one important caveat here, however. Ultrahazardous activity claims are state law tort claims, but Olympus Technologies, as a foreign defendant, could seek to move the case to federal court instead. This means that federal procedural law would govern the case, but California law on torts governs substantive issues relating to what must be proven.[46] Additionally, any challenge to jurisdiction is decided according to state law even if removed to federal court.[47]

There have now been several cases brought against Israeli spyware company NSO Group in California. In *WhatsApp v. NSO Group*, NSO Group tried to dismiss the case on forum non conveniens, among other grounds.[48] Under this doctrine, even when a court does have jurisdiction, it can still dismiss a case if another country also has jurisdiction and it would be more convenient for the parties to litigate there.[49] It is the defendant who must prove that there is an adequate alternative forum and that the balance of private factors (such as residence of the parties, location of witnesses, access to physical evidence, costs of trial, and others) and public factors (like local interest in the case and burden on local juries) is in their favor.[50]

Since NSO Group, like Olympus Technologies, is based in Israel, that was the alternative forum considered in that case. The court ruled, as many others have, that Israel is an adequate alternative forum.[51] That is unlikely to change. Regarding residence of the parties and witnesses, the split in that case was somewhat similar to the one here: The plaintiffs and their witnesses reside in California while the defendant and its witnesses reside in Israel.[52] The case here would be more

41. Pierce, 166 Cal. App. 3d at 85.
42. CACI No. 460, 371.
43. Vast Vantages, LLC v. Bhandari, No. 2:21-cv-04896, 2021 U.S. Dist. LEXIS 220379, at *2–3 (C.D. Cal. 2021); Int'l Shoe Co. v. Wash., 326 U.S. 310 (1945).
44. Goodyear v. Brown, 564 U.S. 915, 919, 924 (2011); Daimler AG v. Bauman, 571 U.S. 117, 122 (2014).
45. Vast Vantages, LLC, 2021 U.S. Dist. LEXIS 220379 at *3–4.
46. US Constitution Annotated, "Art III.S2.C1.16.6 State Law in Diversity Cases and the Erie Doctrine," Congress.gov, n.d., https://constitution.congress.gov/browse/essay/artIII-S2-C1-16-6/ALDE_00013246/, last accessed July 18, 2025.
47. Daimler AG, 571 U.S. at 125.
48. WhatsApp Inc. v. NSO Grp. Techs. Ltd., No. 19-cv-07123, 2023 U.S. Dist. LEXIS 204928 (N.D. Cal. Nov. 15, 2023).
49. Ibid, *3.
50. Ibid, *3–4.
51. Ibid, *5.
52. Ibid, *5–6.

complicated by the fact that Marie is in France and Iris is in the UK. Regarding costs, for plaintiffs costs would be less in California and for defendants they would be less in Israel, so that was not a determining factor.[53] On local interest in the lawsuit, NSO Group argued that Israel's interest "substantially" outweighed California's, but the plaintiffs argued that "California has an interest in providing a means of redress to tortiously injured citizens."[54] The court ruled that both California and Israel had substantial interests, and "at most" this factor only "slightly" favored defendants.[55] Additionally, the case against NSO Group was brought under US federal and California state law, meaning a California court would be far more familiar with it.[56] In the end, most factors were neutral and the only one that was strong, a California court's familiarity with California state and US federal law, favored plaintiffs, so the court denied the motion to dismiss.[57] That analysis would be very similar in Pablo, Iris, and Marie's case.

Sophia highlights another case, one featuring individual victims: *Dada v. NSO Group*, a case brought by journalists from a news organization in El Salvador who alleged their iPhones (produced by Apple, a California company) had been targeted by NSO Group with Pegasus.[58] In that case, none of the plaintiffs lived or worked in California, most were located in El Salvador, but one was a US citizen and two were US residents.[59] The trial court granted NSO's request to dismiss the case on forum non conveniens grounds in March 2024.[60] In July 2025, however, that decision was overturned on appeal.[61]

The appeals court explained that when plaintiffs are both foreign (from another country) and domestic (US citizen or resident), the domestic plaintiff's choice of where to bring the case is still heavily favored and the presence of the foreign plaintiffs does not dilute that.[62] If a domestic plaintiff brings a case somewhere they do not live, they are still entitled to more deference than someone who is foreign but less deference than someone that lives there.[63] Because Pablo is a California resident, he would receive the highest level of deference on his choice of forum and the presence of Marie and Iris would not lessen that. Sophia explains that the appeals decision is unpublished, so they could not cite to it in any future brief, but they could cite the same established cases the appeals court relied on.[64]

What kind of redress is possible?

Regarding damages, Sophia explains that money damages are available for compensation, that is, to cover actual and future expenses. Punitive damages are available if the activities involve malice, oppression, or fraud.[65] For example, in the *WhatsApp v. NSO Group* case, the jury awarded the plaintiff over $400,000 in compensatory damages and over $167,000,000 in punitive damages.[66] But Sophia cautions them not to jump to damages yet. Their case faces an uphill battle and there is no guarantee it will reach a jury or that a jury would even issue punitive damages. The defendants may even offer a settlement. Seeing their vehement reaction, Sophia observes that while they may be against a settlement now, if they are still involved in litigation ten years later, they may feel differently. The important thing to focus on at this stage is, knowing the possibilities, whether the possible risks to them as individuals, including the time and mental health toll, are worth it.

UK

Iris, Marie, and Pablo also meet with Winston, hoping to see whether bringing a case in the UK could be better for them; after all, that is where Iris lives. Winston explains that, unfortunately, when it comes to abnormally dangerous activities, it does not appear that such a case would be successful in the UK due to differences in the development of the doctrine in the two countries over time.

It was a UK case, *Rylands v. Fletcher*, in which water burst from a reservoir a defendant had built and caused damage on nearby property, that is often cited as the origin of the doctrine

53. Ibid, *8.
54. Ibid, *10.
55. Ibid.
56. Ibid.
57. Ibid, *12.
58. See "Dada v. NSO Group," Knight First Amendment Institute at Columbia University, n.d., https://knightcolumbia.org/cases/dada-v-nso-group, last accessed July 18, 2025.
59. *Dada v. NSO Grp. Techs*. Ltd., No. 3:22-cv-07513 2024 U.S. Dist. LEXIS 41261, at *2 (N.D. Cal. Mar. 8, 2024); Dada v. NSO Grp. Techs. Ltd., No. 24-2179, 2025 U.S. App. LEXIS 16647, at *3 (9th Cir. July 8, 2025) (unpublished).
60. Dada, 2024 2024 U.S. Dist. LEXIS 41261.
61. Dada, 2025 U.S. App. LEXIS 16647.
62. Ibid, *4.
63. Ibid, *5.
64. Cal. R. Ct. 8.1115.
65. Frye v. Martinez Refin. Co. LLC, No. 24-cv-04506, 2024 U.S. Dist. LEXIS 229576, at *9, (N.D. Cal. Dec. 16, 2024) (citing Cal. Civ. Code § 3294(a)).
66. Franceschi-Bicchierai, "NSO Group Must Pay More than $167 Million in Damages to WhatsApp for Spyware Campaign."

on strict liability for ultrahazardous activities.[67] However, unlike in the United States, the English judiciary has over time drastically narrowed the scope of applicability of this kind of action to cases typically involving a defendant who is "a land occupier engaging in a land-based activity" and a plaintiff who is "usually a neighboring land occupier complaining about harm to land or structures."[68] Such a strict focus on land and danger based on something "escaping" from the defendant's property to that of another, thus causing physical harm, severely limits the kinds of cases that can be brought under this theory.[69]

It is apparent even just from this basic definition that spyware-related cases would be very unlikely to succeed. For example, even ignoring the elements regarding land, it is hard to argue that spyware "escapes" when it is specifically directed at an individual. Additionally, English courts have limited the kinds of damages that can be recovered in these cases to damages to property.[70] Plaintiffs likely could not recover damages for death or personal injury.[71] Lastly, it seems English courts feel that strict liability for abnormally dangerous activities is better dealt with by lawmakers in Parliament rather than through the courts, demonstrating a reluctance to expand the doctrine.[72] Given the difficulties, including in what kind of damages can even be recovered, Winston advises them to not pursue a case based on strict liability for abnormally dangerous activities in the UK. He says he would carry out further research to see what kinds of other cases could be more productive in the UK.

67. American Law Institute, "Strict Liability," 232.

68. Ibid, 233.

69. See, e.g., Stannard (t/a Wyvern Tyres) v. Gore, [2012] 3 EGLR 129 (summarizing the rule from *Rylands*); Union of India v. Prabhakaran Vijaya Kumar and Others, [2009] 2 LRC 13.

70. Read v. J Lyons & Co Ltd, [1946] 2 All ER 471, 475-76.

71. Transco plc (formerly BG plc and BG Transco plc) v. Stockport Metropolitan Borough Council, [2004] 4 LRC 314, 24. Cf. Perry v. Kendricks Transport Ltd, [1956] 1 All ER 154, 161.

72. See, e.g., Cambridge Water Co. Ltd v. Eastern Counties Leather plc, [1994] 1 LRC 619.

Members of the Judiciary arrive at Westminster Abbey in London. REUTERS/PA Images

Conclusion

Pursuing accountability for spyware abuses is an ongoing challenge. Efforts centered on creating binding regulation and international norms led by states are commendable, but cannot be considered the only path forward. Civil liability plays an important gap-filling function that should be pursued in parallel. As recent cases have demonstrated, while litigation is difficult and resource-intensive, and has a significant impact on the lives of victims and survivors who initiate it, it also offers the possibility of bringing actors responsible for abuses to court, exposing abusive practices, and offering some kind of redress.

Civil liability offers many avenues and strict liability for abnormally dangerous activities is only one possibility. If successful, it could provide significant benefits to possible plaintiffs such as reducing the burden of proof and the number of elements that must be shown. However, as the report shows, even the same theory of liability is applied differently by courts in different jurisdictions. While in California the theory appears to be more promising as a novel legal recourse, the same cannot be said for the UK. Nevertheless, any novel approach to expand an existing legal doctrine carries significant risk but the information herein can help better inform such decisions. As spyware abuses continue to be documented, and regulatory efforts drag on, it is imperative to explore avenues for accountability available now. This report contributes to that dialogue by proposing a theory that has yet to be tested and exploring the possible opportunities and drawbacks to help shape future legal strategies.

Acknowledgements

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. The author also thanks colleagues at the Strategic Litigation Project for research assistance and the following individuals for providing thoughtful feedback: Nadine Farid Johnson, Celeste Kmiotek, Natalia Krapiva, Jen Roberts, Nushin Sarkarati, and Nikita Shah. All errors are the author's own.

Author

Lisandra Novo is senior law and tech advisor for the Atlantic Council's Strategic Litigation Project.

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