



# Any means necessary: Are courts safe in the digital age?

## About this issue brief

Written by  
Lisandra Novo

## Bottom lines up front

- Threat actors have breached the US federal court system multiple times, stealing sensitive sealed materials such as the identities of confidential informants and witnesses.
- Spyware cases pose an increased risk of unauthorized access to sensitive information disclosed in discovery, including how tech companies and forensic research labs detect spyware operations, and the identities of targeted individuals.
- Modern cybersecurity protocols must be paired with non-technical approaches to protect sensitive information.

## Executive summary

When the world's most sophisticated hacking tools are in the hands of those accused of breaking the law, how safe is the justice system itself? What was long a hypothetical scenario fit for a legal thriller is now a repeat occurrence. Since 2020, there have been various reported hacks of the case filing system used by federal courts in the United States.<sup>1</sup> Hacking groups stole sensitive data, including highly sensitive,

sealed materials like the identities of confidential informants or witnesses in cases against drug cartels.<sup>2</sup>

Similar scenarios come to mind reading Apple's explanation for why it voluntarily wanted to end its case against spyware maker NSO Group in 2024, which it called "amoral 21st century mercenaries" in its initial complaint just three years earlier.<sup>3</sup> WhatsApp, on the other hand, continued its own case against the same group and secured a multimillion-dollar victory despite facing the

1. John Sakellariadis, "Hack of Federal Court Filing System Exploited Security Flaws Known Since 2020," *Politico*, August 12, 2025, <https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392>.
2. Ibid.; Josh Gerstein, "Federal Court Filing System Hit in Sweeping Hack," *Politico*, August 6, 2025, <https://www.politico.com/news/2025/08/06/federal-court-filing-system-pacer-hack-00496916>.
3. Plaintiff Apple Inc.'s Motion for Voluntary Dismissal Under Fed. R. Civ. P. 41(a)(2) at 2-4, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078-JD (N.D. Cal. Sept. 13, 2024), ECF No. 98 [hereinafter Apple Motion for Dismissal]; Complaint at 1, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 5:21-cv-09078 (N.D. Cal. Nov. 23, 2021), ECF No. 1 [hereinafter Apple Complaint].

same discovery threats.<sup>4</sup> Due process demands that a litigant have the right to be heard about key issues in a case; building a secretive system that destroys that right is not the answer.

Existing protective measures, such as limiting access to evidence only to attorneys involved in the litigation, are extremely valuable but vulnerable to sophisticated threats. These measures can be complemented by additional security and strategic steps to make them fit for the digital age. Technical solutions like strong cybersecurity practices are essential but must be paired with non-technical solutions such as time-limited, on-premises access to physical documents, litigation strategies that center non-technical evidence, stressing the relevance of specific evidence to material questions, and clearly explaining thresholds for the applicable standard of proof. Lastly, lawmakers can enact rules to shield victims' identities, guarantee confidentiality, and incentivize ongoing security research.

### ■ Recommendations

These recommendations are based on existing structures and cases in the United States, but many can serve as useful starting points for other jurisdictions.

Policymakers should ensure, at a minimum, that judiciary systems are employing basic cybersecurity practices and have clear data access protocols for sensitive information.

Policymakers should explore non-technical solutions for sealed materials, such as on-premises access for physical documents that are not entered into digital case management systems until a specified date.

While accounting for due process concerns, policymakers should prioritize statutory frameworks designed to protect the confidentiality of victims who work with security researchers. These frameworks should employ neutral definitions of security research and researchers that do not depend on institutional affiliation.

Established research labs should share guidance on ethics, confidentiality, and research best practices to protect research subjects with newly established threat labs, rapid response or-

ganizations, and other entities that provide forensic assistance to targeted individuals.

To best meet classification definitions, researchers at entities other than traditional research institutions like universities should take care to separate their work and organization structure.

Relevant stakeholders such as policymakers, judges, litigators, investigators, and affected individuals should engage in thorough debate about the kinds of appropriate technical and non-technical evidence for showing unauthorized access and attributing it to a particular actor.

Journalists, academics, and other experts covering spyware or surveillance cases should make clear that a "smoking gun" forensic report is not necessary and explain the relevant thresholds for proving claims in civil and criminal litigation (i.e., more likely than not or beyond a reasonable doubt). Such nuanced coverage can feed larger discussions about the kinds of evidence necessary to prove material questions in these cases.

Professional associations should host continuing education sessions or special workshops to update judges, lawyers, and law enforcement about the intricacies of cases turning on technical evidence.

### ■ Introduction

Apple has been sending threat notifications since 2021 to users in more than 150 countries who have been targeted by sophisticated "mercenary spyware attacks."<sup>5</sup> This was the same year Apple filed its complaint against NSO Group, alleging that the spyware maker violated US federal and state laws through "egregious, deliberate, and concerted efforts . . . to target and attack Apple customers, Apple products and servers and Apple through dangerous malware and spyware."<sup>6</sup> On its own support page, Apple explains that users are typically targeted "because of who they are or what they do" and that these attacks are extremely sophisticated "as mercenary spyware attackers apply exceptional resources to target a very small number of specific individuals and their devices," with attacks typically costing millions of dollars.<sup>7</sup>

---

4. Tim Starks, "Judge Forbids NSO Group from Targeting WhatsApp Users," Cyberscoop, October 20, 2025, <https://cyberscoop.com/whatsapp-wins-injunction-against-nso-group-spyware-damages-reduced/>.

5. "About Apple Threat Notifications and Protecting Against Mercenary Spyware," Apple, last updated August 13, 2026, <https://support.apple.com/en-us/102174>.

6. Apple Complaint at 2.

7. "About Apple Threat Notifications and Protecting Against Mercenary Spyware."

In August 2025, Apple sent out alerts to users in 110 countries.<sup>8</sup> Alerts were sent directly through an Apple threat notification on the iPhone's lock screen and settings page, an email, and a notification banner on the user's account page.<sup>9</sup> The threat notifications also advised users about what actions to take, such as turning on Apple's Lockdown Mode and seeking expert help.<sup>10</sup> To protect against revealing how the threat alert program and internal security research discover such intrusions, Apple moved to voluntarily dismiss its own case against NSO Group in September 2024.<sup>11</sup>

But how does civil litigation endanger security research and assistance? What happened to make Apple go from vigorously asserting its case against a group it called "amoral 21st century mercenaries" responsible for creating "highly sophisticated cyber-surveillance machinery that invites routine and flagrant abuse" to feeling like its entire security research program was endangered by continuing its case?<sup>12</sup> The answer lies in a complicated legal web and a rapidly changing cybersecurity reality.

### ■ A tale of two legal dramas

In Apple's case, NSO Group argued that there were legal developments in Israel that could potentially complicate discovery in the case before US courts.<sup>13</sup> It is difficult to know exactly what these developments were because the publicly available

documents are heavily redacted.<sup>14</sup> Importantly, the judge noted that Apple itself rebutted NSO's claims by saying, as recently as October 2023, that discovery would not be so burdensome, "particularly with use of protective orders and judicial oversight."<sup>15</sup> Yet, eleven months later, Apple asked the court to dismiss its own case because it feared no protective measure would be enough to mitigate the risks of any disclosure.<sup>16</sup>

Apple's first claim was that "adversaries aggressively seek" information about its security protections for its users worldwide, "using any means necessary."<sup>17</sup> Apple next claimed that NSO Group was no longer the most significant player in an ever-growing spyware ecosystem, meaning that any reward for Apple continuing the litigation paled in comparison to the risk of any spyware company seeking out the information, even if it were sealed.<sup>18</sup> Lastly, Apple claimed that NSO's conduct in the case brought by WhatsApp signaled it could attempt to avoid needing to produce its own information in the Apple case.<sup>19</sup>

In its reply, NSO Group pointed out that "the exchange of information in discovery is simply a requirement in civil litigation in the United States."<sup>20</sup> Apple, and any other US litigant, would likely agree. NSO also argued that Apple was irresponsible in suggesting that "NSO, its counsel, or anyone else would fail to preserve the security of Apple's confidential material."<sup>21</sup> In assessing this statement, it is important to note NSO's own mar-

8. Zack Whittaker, "If Apple Sends You a Push Notification Alerting You to a Spyware Attack, Take It Seriously," TechCrunch, August 13, 2026, <https://techcrunch.com/2026/08/13/if-apple-sends-you-a-push-notification-alerting-you-to-a-spyware-attack-take-it-seriously/>.
9. "About Apple Threat Notifications and Protecting Against Mercenary Spyware."
10. Ibid.
11. Apple Motion for Dismissal.
12. Apple Complaint at 1-2; Apple Motion for Dismissal at 2-4.
13. Defendant NSO Group Technologies Ltd. And Q Cyber Technologies Ltd.' Supplemental Memorandum in Support of Renewed Motion to Dismiss at 2-3, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078-JD (N.D. Cal. Oct. 12, 2023), ECF No. 74 [hereinafter NSO Supplemental Memorandum]; *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078-JD, slip op. at 5 (N.D. Cal. Jan. 23, 2024), ECF No. 87 [hereinafter Apple v. NSO Order re Motion to Dismiss].
14. See, e.g., NSO Supplemental Memorandum 2; Plaintiff Apple Inc.'s Opposition to Defendants' Supplemental Memorandum in Support of Their Renewed Motion to Dismiss at 4, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078-JD (N.D. Cal. Oct. 19, 2023), ECF No. 75 [hereinafter Apple Opposition to NSO Supplemental Memorandum].
15. Apple v. NSO Order re Motion to Dismiss at 5; Apple Opposition to NSO Supplemental Memorandum at 3-4.
16. Apple Motion for Dismissal at 3.
17. Ibid.
18. Ibid at 3-4.
19. Ibid at 4.
20. Defendants' Statement in Response to Plaintiff's Motion for Voluntary Dismissal Without Prejudice at 7, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078-JD (N.D. Cal. Sept. 27, 2024), ECF No. 100 [hereinafter NSO Response to Apple Motion for Dismissal].
21. Ibid at 8.

keting materials highlight tools it developed precisely to get around security measures safeguarding private information.<sup>22</sup>

NSO Group also rebutted Apple's reliance on a *Guardian* article about measures the Israeli government took to allegedly prevent NSO Group from complying with discovery orders in the WhatsApp case.<sup>23</sup> NSO maintained it never shared materials with anyone "not allowed to receive" them and that the material allegedly seized by Israel belonged only to NSO, not to Apple.<sup>24</sup> The article reported that Israeli authorities seized documents and computers from NSO offices in July 2020 after supposedly discussing with company officials how to respond to discovery orders issued by the judge in the WhatsApp case. The seizure itself was under a gag order issued by an Israeli court, a copy of which was later obtained by journalists.<sup>25</sup>

Those allegations did not go unnoticed in the WhatsApp case. In a motion calling for sanctions on NSO Group, WhatsApp relied on the *Guardian* article twice in another heavily redacted document in which it argued that "NSO deliberately took steps to impede Plaintiffs' access to relevant discovery . . . that the Court had specifically ordered NSO to produce."<sup>26</sup> WhatsApp's lawyers also argued that they specifically asked NSO to respond to allegations in the reporting that one of its lawyers allegedly reached out to the Israeli government to ask for help in avoiding needing to comply with the court's discovery orders, including for the Pegasus source code.<sup>27</sup> NSO's response was

that the article's claim that it asked the Israeli government to "rescue" it was not about discovery but rather a "conversation" asking the Israeli government to request that the US State Department ask for the case to be dismissed altogether.<sup>28</sup> NSO's counsel further argued that there had been a "massive effort by the defendants to comply with the court's orders," with NSO having "produced 50,000 pages of technical material."<sup>29</sup>

It is not a wild leap to think some threat actors would target US courts to get confidential information, such as the source code of a rival spyware maker; state-affiliated hacking groups have already done so multiple times.<sup>30</sup> Faced with the same threats as Apple, both WhatsApp and NSO nevertheless produced extensive amounts of information, even considering the court's rebuke that NSO engaged in "pure gamesmanship" and failed to comply with discovery orders to turn over "key facts at issue" in the case, notably Pegasus source code.<sup>31</sup> Both WhatsApp and NSO Group made numerous motions for protective measures for the material provided.<sup>32</sup> As NSO's counsel highlighted in one such request, courts in California—where many tech-related cases are brought—"routinely seal confidential and sensitive competitive information . . . concerning technology or descriptions of such technology."<sup>33</sup> The court granted many of these requests, allowing sensitive but key material to be either redacted or filed completely under seal, such as the document showing the number of times "Pegasus code

- 
22. "Inside Pegasus: The Evolution of the World's Most Notorious Spyware System," Amnesty International Security Lab, July 16, 2026, <https://securitylab.amnesty.org/latest/2026/07/inside-pegasus-the-evolution-of-the-worlds-most-notorious-spyware/>.
  23. NSO Response to Apple Motion for Dismissal at 7-8; Harry Davies and Stephanie Kirchgaessner, "Israel Tried to Frustrate US Lawsuit over Pegasus Spyware, Leak Suggests," *Guardian*, July 25, 2024, <https://www.theguardian.com/news/article/2024/jul/25/israel-tried-to-frustrate-us-lawsuit-over-pegasus-spyware-leak-suggests>.
  24. NSO Response to Apple Motion for Dismissal at 7-8.
  25. Davies, and Kirchgaessner, "Israel Tried to Frustrate US Lawsuit over Pegasus Spyware, Leak Suggests."
  26. Plaintiffs' Notice of Motion and Motion for Sanctions at 24-25, *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, No. 4:19-cv-07123-PJH (N.D. Cal. Oct. 2, 2024), Dkt. No. 406.
  27. Transcript of Proceedings Before the Honorable Phyllis J. Hamilton at 84-85, *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, No. 4:19-cv-07123-PJH (N.D. Cal. Nov. 7, 2024), Dkt. No. 464 [hereinafter Transcript of WhatsApp November 2024 Hearing].
  28. *Ibid* at 91.
  29. *Ibid* at 92.
  30. Mattathias Schwartz, "Federal Courts Slow to Fix Vulnerable System after Repeated Hacking," *New York Times*, September 3, 2025, <https://www.nytimes.com/2025/09/03/us/politics/federal-courts-computer-hacks.html>.
  31. Transcript of WhatsApp November 2024 Hearing at 88; *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, No. 4:19-cv-07123-PJH, slip op. at 9 (N.D. Cal. Dec. 20, 2024), Dkt. No. 494 [hereinafter WhatsApp Order re Summary Judgment and Discovery Sanctions].
  32. A search for the word "seal" in the docket yields hundreds of results. "WhatsApp Inc. v. NSO Group Technologies Limited (4:19-cv-07123)," CourtListener, last visited September 18, 2026, <https://www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/>.
  33. Declaration of Aaron S. Craig in Support of Defendants NSO Group Technologies Limited and Q Cyber Technologies Limited's Administrative Motion to File Under Seal at 10, *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, No. 4:19-cv-07123-PJH (N.D. Cal. Oct. 11, 2024), Dkt. No. 419-8.

was sent through plaintiffs' California-based servers," which remains unavailable to the public at the time of writing.<sup>34</sup>

### ■ Protective measures guarantee due process

Discovery in US litigation presents opportunities for getting information from the other party that might be essential to the case, but it also carries significant risk of needing to disclose information that goes against a party's interests outside the litigation.<sup>35</sup> Recognizing these risks, US courts have some discretion to issue protective orders.<sup>36</sup> For example, in trades secrets cases in which showing certain information to the other party could be an existential business risk, there is a statutory framework available to ensure confidentiality, primarily through the use of protective measures.<sup>37</sup>

When issued, protective measures allow for certain information to be revealed only in a specific way or not at all.<sup>38</sup> However, even in trade secrets cases, this protection is not automatic and a party seeking it needs to show why it is warranted, as the public's right to access court filings is the starting presumption.<sup>39</sup> The court also considers the other party's interest in this information and how relevant it is to its case.<sup>40</sup> If issued, protective orders can cover all discovery or only specific information, or can allow a party to determine in good faith what should be protected.<sup>41</sup> Additionally, courts can set limits on who is allowed to see the protected information. The looser level prevents third parties from seeing the information but allows the parties to the litigation to do so; the strictest level, commonly called an

"attorneys' eyes only" designation, allows only legal counsel—but not the party itself—to see the information.<sup>42</sup>

Protective orders are not absolute. They are not permanent and a judge can reverse or modify them at their discretion.<sup>43</sup> Additionally, even the strictest level of confidentiality, an "attorneys' eyes only" designation, does not shield the information from the opposing party's legal counsel.<sup>44</sup> When necessary, judges can conduct private examination (*in camera* review) of specific information to determine whether it merits protection.<sup>45</sup> The Code of Conduct for United States Judges, for example, stresses that judges "should accord to every person who has a legal interest in a proceeding, and that person's lawyer, the full right to be heard according to law," meaning that—aside from extremely limited exceptions—"a judge should not initiate, permit, or consider *ex parte* communications or consider other communications concerning a pending or impending matter that are made outside the presence of the parties or their lawyers."<sup>46</sup> A judge's private review of material provided by one side without the other party's involvement (*ex parte*) is even more exceptional and typically occurs in national security cases in which exceptions provided by law apply.<sup>47</sup>

### ■ Is there a way forward?

Breaking long-standing rules that seek to guarantee a party's right to be heard by expanding secret, one-sided review of material evidence is not the solution, nor would it prevent unauthorized access. The Administrative Office of the US Courts acknowledged in 2025, after reporting on the major hacks to

34. WhatsApp Order re Summary Judgment and Discovery Sanctions at 6.

35. Natalia Krapiva, "Discovery in U.S. Spyware Litigation: A Double-Edged Sword?" Just Security, August 19, 2025, <https://www.just-security.org/118409/discovery-spyware-double-edged-sword/>.

36. Fed. R. Civ. P. 26(c).

37. 18 U.S.C.A. § 1835 (a).

38. Fed. R. Civ. P. 26(c)(1)(G).

39. See, e.g., *Smith v. BIC Corp.*, 869 F.2d 194, 199-201 (3d Cir. 1989); *Federal Open Market Committee of Federal Reserve System v. Merrill*, 443 U.S. 340, 362 (1979); N.D. Cal. Civil L.R. 79-5(a).

40. *Bridgestone Americas Holding, Inc. v. Mayberry*, 878 N.E.2d 189, 193 (Ind. 2007).

41. *Gillard v. Boulder Valley School Dist. Re.-2*, 196 F.R.D. 382, 385-86 (D. Colo. 2000).

42. See *Layne Christensen Co v. Purolite Co.*, 271 F.R.D. 240, 246 (D. Kan. 2010).

43. See *Pansy v. Borough of Stroudsburg*, 23 F.3d 772,784 (3d Cir. 1994).

44. See *Silversun Industries, Inc. v. PPG Industries, Inc.*, 296 F.Supp.3d 936, 947 (N.D. Ill. 2017).

45. See, e.g., *Woven Electronics Corp. v. Advance Group, Inc.*, 930 F.2d 913 (Table) (4th Cir. 1991).

46. "Code of Conduct for United States Judges," United States Courts, last updated March 12, 2019, <https://www.uscourts.gov/administration-policies/judiciary-policies/ethics-policies/code-conduct-united-states-judges>.

47. See, e.g., David Greene, "Jewel v. NSA: Making Sense of a Disappointing Decision over Mass Surveillance," Electronic Frontier Foundation, February 11, 2015, <https://www EFF.org/deeplinks/2015/02/jewel-v-nsa-making-sense-disappointing-decision-over-mass-surveillance>.

federal court systems, that sensitive documents containing “confidential or proprietary information that are sealed from public view . . . can be targets of interest to a range of threat actors.”<sup>48</sup> The office reiterated its commitment to “enhancing” security and recalled steps that had already been implemented, such as expanding multifactor authentication and limiting use of personal, nongovernment devices to access sensitive information.<sup>49</sup> Future technical steps should include standardizing redaction processes by courts and parties to ensure text cannot be extracted from materials when it is made public.<sup>50</sup> These are the bare minimum steps and, according to critics like Senator Ron Wyden, many were available for years before the judiciary adopted them.<sup>51</sup> Wyden of Oregon and Senator John Kennedy of Louisiana have reintroduced a bipartisan bill to make necessary efficiency and cybersecurity updates to federal court filing systems.<sup>52</sup>

Technical measures cannot be the only solution to securing highly sensitive material. The market for vulnerabilities continues to expand and new AI models make it easier for an increasing variety of actors to find them.<sup>53</sup> To go forward, the answer might involve going backward: the safest solution might sometimes be physical on-premises access so that some documents do not enter the digital system in the first place until a specified date at which point it is safe to grant public access, even if to redacted documents. Such a drastic solution would need additional safeguards such as physical location

security, access policies, measures to ensure litigants—especially future litigants unrelated to the specific case—and their counsel can adequately access items necessary for case preparation, and balancing against the public’s interest in accessing these materials.

For the most sophisticated cyber surveillance capabilities, such as spyware, even these measures might not be enough. US courts have long acknowledged that confidentiality is essential for researchers and that any threat to the promise of confidentiality from potential disclosure must be weighed against society’s interest in accessing the results.<sup>54</sup> Courts have also recognized the chilling effect that being dragged into litigation can have on researchers who were not involved in the dispute but might possess material relevant to the litigation.<sup>55</sup> But protective orders are not absolute and therefore face the same obstacles discussed above.<sup>56</sup>

A system currently available for health-related research could provide a starting point for protecting the most sensitive information: identities of individuals affected by spyware. The Comprehensive Drug Abuse Prevention and Control Act of 1970, building off the Public Health Service Act of 1944, guarantees that researchers engaged in health-related research could “not be compelled” to disclose the names or other identifying information of research subjects.<sup>57</sup> This statutory protection has been expanded several times, responding to

- 
48. “Cybersecurity Measures Strengthened in Light of Attacks on Judiciary’s Case Management System,” United States Courts, August 7, 2025, <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>.
  49. Ibid.; “Judicial Conference Briefed on the Need for Continued Vigilance on Cybersecurity and Workplace Conduct,” United States Courts, September 17, 2024, <https://www.uscourts.gov/data-news/judiciary-news/2024/09/17/judicial-conference-briefed-need-continued-vigilance-cybersecurity-and-workplace-conduct>.
  50. See, e.g., Davey Winder, “Hackers Unredact Epstein Files—What You Need to Know,” *Forbes*, December 26, 2025, <https://www.forbes.com/sites/daveywinder/2025/12/26/epstein-files-hacked---all-you-need-to-know/>.
  51. Tim Starks, “Blistering Wyden Letter Seeks Review of Federal Court Cybersecurity, Citing ‘Incompetence,’ ‘Negligence,’” *CyberScoop*, August 25, 2025, <https://cyberscoop.com/blistering-wyden-letter-seeks-review-of-federal-court-cybersecurity-citing-incompetence-negligence/>.
  52. “Kennedy, Wyden Introduce Bipartisan Bill to Modernize Federal Court Records System,” John Kennedy, US Senator for Louisiana, press release, June 2, 2026, <https://www.kennedy.senate.gov/public/2026/6/kennedy-wyden-introduce-bipartisan-bill-to-modernize-federal-court-records-system>.
  53. Varun Badhwar, “AI Is Commoditizing Vulnerability Discovery Faster Than Organizations Can Respond,” *Forbes*, September 4, 2026, <https://www.forbes.com/councils/forbestechcouncil/2026/09/04/ai-is-commoditizing-vulnerability-discovery-faster-than-organizations-can-respond/>.
  54. See, e.g., *Andrews v. Eli Lilly & Co., Inc.*, 97 F.R.D. 494, 499-502 (N.D. Ill. 1984).
  55. See, e.g., *Cusumano v. Microsoft Corp.*, 162 F.3d 708, 717 (1st Cir. 1998).
  56. *Federal Open Market Committee of Federal Reserve System v. Merrill*, 443 U.S. 340, 362 (1979).
  57. Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, Part E, § 3(a), (1970).

significant public health concerns at the relevant time.<sup>58</sup> Not only do certificates of confidentiality prevent the disclosure of this identifying information (save in extremely limited circumstances), but the protection granted is permanent and can even be retroactive.<sup>59</sup>

In simple terms, under the health research confidentiality certificate system, a researcher makes a request to the appropriate Health and Human Services agency through an online application.<sup>60</sup> The researcher must provide certain administrative information, such as the project details, the institution where the research will be carried out, and who the principal investigator will be.<sup>61</sup> Crucially, this protection applies only to identifying information of research subjects and not to other elements of the research such as methodology.<sup>62</sup>

The suggestion to create a framework for comparable certificates of confidentiality for security researchers raises more questions than it answers. Would a system need to be set up in each country where researchers are located? Under what agency? What protection would be afforded to research conducted in other countries? How would researchers be defined? Would they need to be affiliated with a university? Such a requirement would exclude Apple's own threat team as well

as many rapid response organizations that provide forensic assistance to individuals targeted by spyware or other malware. Political will is key to designing and enacting this kind of system. The one for health research in the United States can be traced back to the 1940s with decades between expansions, each of which responded to pressing societal concerns.

Lastly, this system does not provide blanket confidentiality for research methodology—ostensibly what Apple felt was needed to continue its litigation. But that is an overbroad request that ignores the role of lawyers in crafting a holistic case, the standard a party must meet for proving its case, and the effect creating one system for unlikeable defendants would have on all defendants. It also overemphasizes the centrality of technical documentation, which is difficult for judges and juries to understand, and which typically points to patterns suggesting a particular actor might be responsible to a certain degree of certainty. Parties in civil litigation can certainly meet the threshold of a preponderance of the evidence (colloquially referred to as a 51 percent probability) using material that is safe to disclose without endangering whole programs of research. This is a reminder that the answer to technical problems does not always lie in technical solutions.

---

58. H.R. Rep. No. 91-1444, 4566, 4572-74 (1970); S. Rep. 100-133, 1, 4-7 (1987); Elonna Ekweani, Taunton Paine, and Kate Tapley, *Certificates of Confidentiality Following Enactment of the 21st Century Cures Act*, 11(3) J. Health Life Sci. L. 1, 2-4 (2018); Leslie E. Wolf et al., *Certificates of Confidentiality: Privileging Research Data*, 11 J. of L. and the Biosciences, 1, 4-5 (2024).

59. 42 U.S.C. § 241(d); *SACHRP Recommendations, Attachment B: Recommendations of Certificates of Confidentiality*, U.S. Department of Health and Human Services (2014).

60. 42 U.S.C. § 241(d)(1)(A); *SACHRP Recommendations, Attachment B*.

61. *SACHRP Recommendations, Attachment B*.

62. *Wolpin v. Philip Morris Inc.* 189 F.R.D. 418, 425 n.4 (C.D. Cal. 1999).

---

## About the author

Lisandra Novo is the senior law and tech adviser for the Strategic Litigation Project (SLP).

The author would like to acknowledge the excellent research assistance provided by SLP's junior legal fellow and the peer reviewers' thoughtful feedback. All errors are the author's own.

---

## About the centers

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.