
A STATUTORY SOLUTION TO STORAGE SHORTFALLS IN CHILD SEXUAL ABUSE MATERIAL INVESTIGATIONS

Jessica L. Terkovich*

I. INTRODUCTION

Investigators caught Richard Belden, a man from Collin County, Texas, with fifty-eight terabytes of child sexual abuse material (“CSAM”)¹ on a total of fifteen hard drives as part of Project Safe Childhood, a nationwide initiative to fight child sexual abuse and exploitation.² Fifty-eight terabytes is approximately 453 iPhones’ worth of data.³ In other terms, fifty-eight terabytes is the equivalent of approximately 58 million photos or 4.7 years of video.⁴ Unfortunately, this nearly incomprehensible amount of CSAM is not atypical in these types of investigations: in February of 2025, the Solano County Sheriff’s Department in California recovered 120 terabytes of CSAM on a total of twenty devices, over double the amount that Belden had been hoarding across his devices.⁵ Even smaller cases often contain tens of thousands of images and hours of video evidence.⁶ All of this CSAM must be viewed and stored in a secure manner by

* Assistant Commonwealth’s Attorney at the Office of the Norfolk Commonwealth’s Attorney in Norfolk, VA. B.A., University of Florida; J.D., University of Florida Levin College of Law.

1. Many statutes refer to this material as “child pornography.” While the author retains this phrasing when quoting directly from a statute, court case, or news media source, all other internal references to this material in the Article will be to “child sexual abuse material” or “CSAM.” The word “pornography” implies the depiction of a consensual sexual act between adults, while “CSAM” is a more victim-centered and trauma-informed term that acknowledges the fact that children fundamentally cannot consent to sexual acts or depictions.

2. Braylee McCoy, *Man Caught with 58 Terabytes of Child Porn Sentenced to 35 years*, KXII NEWS (Feb. 10, 2020, at 5:32 CT), <https://www.kxii.com/content/news/Collin-County-man-sentenced-to-35-years-in-prison-for-possessing-child-pornography-567742771.html> [<https://perma.cc/HB46-4PS5>].

3. *Id.* Using the average 128 gigabytes of storage in the typical iPhone for measure.

4. *See How Big Is 58 Terabytes (TB)? Is It Enough for You?*, FOYER, <https://usefoyer.com/how-big-is-58-terabytes> [<https://perma.cc/9AUP-6HAC>] (last visited Nov. 12, 2025).

5. Cecilio Padilla, *Solano County Sheriff Says 120 Terabytes of Suspected Child Sexual Assault Material Seized in Vallejo*, CBS NEWS (Feb. 24, 2025, at 4:57 PT), <https://www.cbsnews.com/sacramento/news/vallejo-csam-120-terabytes-seized-solano-county-sheriff/> [<https://perma.cc/A48B-KWKH>].

6. *See, e.g., Michigan Man Sentenced to Five Years in Prison for Possessing Child Sexual Abuse Material on a Military Base*, DEP’T OF JUST. (June 13, 2025), <https://www.justice.gov/opa/pr/michigan-man-sentenced-five-years-prison-possessing-child-sexual-abuse-material-military> [<https://perma.cc/BB4L-WUKK>].

investigators to further the investigation into CSAM sources and producers and to prosecute those involved.⁷

The average American household has over twenty internet-connected devices in a broad range of categories, the most ubiquitous of which are cell phones and laptops.⁸ This gives the average person an unlimited ability to connect to the internet for work, school, and entertainment, but it also opens up unlimited possibilities for abuse. Internet Crimes Against Children (“ICAC”) investigative task forces have expanded across the country since their initial federal development in 1998.⁹ Funding for local law enforcement’s ICAC investigative technology, however, has not kept pace with device and data growth, leading to a significant resource gap.¹⁰

One of the most significant challenges to law enforcement agencies is a lack of storage space: given the number of devices that could potentially be seized from a suspect, investigators may need terabytes of storage space that their departments simply cannot afford.¹¹ As a result, investigators struggle to keep up with the amount of incoming tips and the heavy data storage demand of each investigation.¹²

Some states have laws that allow for the forfeiture of devices and external storage drives seized in CSAM cases,¹³ which helps to alleviate the funding gap that investigators would otherwise need to fill themselves, unless they choose to forego the full number of investigations they could pursue. This Article delves into the CSAM-specific forfeiture provisions on the books in these states and how they have the potential to assist investigators in ICAC cases. Part II discusses the investigative techniques used by ICAC task forces and demonstrates the need for additional storage devices not supplied by the governing state, county, or city. Part III discusses the results of a nationwide survey of forfeiture that includes specific provisions for CSAM-related devices and external storage drives. Part IV reviews some local law enforcement policies and procedures employed in states with CSAM-specific forfeiture laws. Finally, Part V concludes by offering recommendations for drafting effective CSAM-

7. *Addressing the Challenges of the ICAC Task Forces: Funding, Education and Legislative Reforms*, CELLEBRITE (May 30, 2024), <https://ofta.cellebrite.com/addressing-the-challenges-of-the-icac-task-forces-funding-education-and-legislative-reforms/> [<https://perma.cc/TNC4-E2RU>].

8. Collin Blinder, *Average Number of Smart Devices in a Home 2025*, CONSUMER AFFS. (Apr. 23, 2024), <https://www.consumeraffairs.com/homeowners/average-number-of-smart-devices-in-a-home.html#devices-by-household> [<https://perma.cc/4N8T-MBYH>].

9. OFF. OF JUV. JUST. & DELINQ. PREVENTION, DEP’T OF JUST., INTERNET CRIMES AGAINST CHILDREN TASK FORCE PROGRAM, <https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program> [<https://perma.cc/X9C2-YAPK>] (last visited Nov. 12, 2025).

10. *Addressing the Challenges of the ICAC Task Forces: Funding, Education and Legislative Reforms*, *supra* note 7.

11. *See, e.g.*, McCoy, *supra* note 2.

12. *Addressing the Challenges of the ICAC Task Forces: Funding, Education and Legislative Reforms*, *supra* note 7.

13. *See, e.g.*, ALASKA STAT. § 11.61.129(a); O.C.G.A. § 16-12-100; 17-A ME. REV. STAT. § 285(1); MD. CRIM. L. CODE § 11-211 (2024); NEV. REV. STAT. 200.760; S.D. REV. STAT. 22-24A-15; TEX. PEN. CODE 59.01(2)(A)(iii); WY. REV. STAT. 6-4-303(f)(iii).

specific forfeiture provisions for states and for local law enforcement agencies looking to address these forfeitures in their policy manuals.

II. INVESTIGATIVE TECHNIQUES

The Internet Watch Foundation had cataloged 132,676 web pages that advertised, linked users to, or contained CSAM by 2019.¹⁴ During a 90-day period in 2024, Raven, an affiliate of investigatory software Cellebrite and a 501(c) 4 group focused on ending child exploitation, logged 99,732 IP addresses that shared “images of infant and toddler rape and abuse,” but only 638 were under investigation, as funding for investigations remained incredibly low.¹⁵ These investigations are time-, labor-, and storage-intensive. This resource gap is especially alarming because children are harmed during production, but also can be harmed by viewers: many individuals who had never sexually abused a child attempt to seek out and sexually abuse children after viewing CSAM.¹⁶ Some estimate this number to be as high as 41.8% of CSAM viewers.¹⁷

A. Opening an Investigation

CSAM cases usually either begin with the arrest of a hands-on offender and the seizure of their devices or with a tip from an Internet Service Provider (“ISP”), social media site, or cloud storage provider.¹⁸ These tips provide information about potential CSAM to investigators and the National Center for Missing and Exploited Children (“NCMEC”), a private entity with the unique statutory obligation to operate the official clearinghouse for information about missing, endangered, and exploited children.¹⁹ NCMEC is charged with helping law enforcement locate and recover missing and exploited children, providing “forensic technical assistance” to law enforcement, helping to identify victims of child exploitation, and operating their CyberTipline.²⁰

14. Benoit Leclerc, *The Case of Child Sexual Abuse Material Online and Crime Script Analysis*, GRIFFITH UNIV. (Nov. 3, 2021), <https://enlighten.griffith.edu.au/the-case-of-child-sexual-abuse-material-online-and-crime-script-analysis/> [<https://perma.cc/M7VX-VUNM>].

15. *Advocates Hold Hill Briefing on the Impact and Cost of Our Exploited Children*, RAVEN (Mar. 2024), <https://raven.us/advocates-hold-hill-briefing-on-the-impact-and-cost-of-our-exploited-children/>.

16. Leclerc, *supra* note 14.

17. Nurmi et al., *Investigating Child Sexual Abuse Material Availability, Searches, and Users on the Anonymous Tor Network for a Public Health Intervention Strategy*, SCI. REPS., 14(1), 7849 (2024), <https://doi.org/10.1038/s41598-024-58346-7> [<https://perma.cc/B6WP-FCF7>].

18. *See id.*; *see also Addressing the Challenges of the ICAC Task Forces: Funding, Education and Legislative Reforms*, *supra* note 7.

19. *U.S. v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016).

20. *Id.* ISPs satisfy legal reporting requirements by sending CyberTipline reports to NCMEC. 18 U.S.C. § 2258A(a)(1). CyberTips usually contain the facts and circumstances regarding an alleged violation of federal laws related to online child exploitation. *Id.* They may also provide information about the individuals involved, geographical location information, known images of CSAM, and other related communications. *Id.* § 2258A(b)(1)–(5).

NCMEC partners with several larger law enforcement and investigative agencies to distribute lists of the hash values of “known” CSAM videos and images to ISPs and smaller law enforcement agencies.²¹ Hash values are strings of numbers and letters generated by an algorithm through which the video or image of CSAM is run.²² This algorithm also assigns a unique identifier to the video or image that can be used to confirm if it is new to investigators or has been discovered previously.²³ When an image or video is run through the hashing algorithm, it will always produce the same hash value, unless something about the image or video has been edited, making it “new.”²⁴ Even an insubstantial edit, such as cropping an image or brightening a video, will change the hash value.²⁵ Some experts liken hash values to the uniqueness of fingerprints.²⁶ If two examiners across the country compute an identical hash value for an image, they know they are looking at the same image, even if the images were seized from different offenders in unique investigations.²⁷

Distributing a list of “known” hash values means that NCMEC and law enforcement agencies are not *actually* sharing CSAM, but still help to further investigations across the country.²⁸ Examiners can use this list of hash values to search seized devices and inspect any flagged content, but they can also add to the list by contacting NCMEC about “new” images and videos that they have discovered.²⁹ This ever-growing list of over five million hash values is distributed to software development, social media, and search engine companies, who are then tasked with notifying NCMEC if they receive any hits in their users’ data.³⁰

B. Device Security and Data Dumps

Once a report has been made, local law enforcement agencies are tasked with arresting the offender and seizing any devices they may be using to create, solicit, distribute, or store CSAM.³¹ Regardless of how the offender came to the

21. See, e.g., *Blocking and Categorizing Content*, INTERPOL, <https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content> [<https://perma.cc/ULK5-R69X>] (last visited Nov. 12, 2025).

22. Jon Berryhill, *What Is a Hash Value?*, BERRYHILL FORENSICS (July 15, 2019), <https://www.computerforensics.com/news/what-is-a-hash-value> [<https://perma.cc/HZU6-G63W>].

23. *Id.*

24. *Id.*

25. NAT’L CTR. FOR MISSING & EXPLOITED CHILD., 2022 NCMEC/OJJDP TRANSPARENCY REPORT 6 n.4 (2022), https://www.missingkids.org/content/dam/missingkids/pdfs/OJJDP-NCMEC-Transparency_2022-Calendar-Year.pdf [<https://perma.cc/P3DA-5J6N>].

26. See Richard Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38–40 (2005).

27. Berryhill, *supra* note 22.

28. *Id.*

29. *Id.*

30. NCMEC, *Google and Image Hashing Technology*, GOOGLE, INC., <https://safety.google/stories/hash-matching-to-help-ncmec/> [<https://perma.cc/FT5S-97KY>] (last visited Nov. 12, 2025).

31. See *Addressing the Challenges of the ICAC Task Forces: Funding, Education and Legislative Reforms*, *supra* note 7.

attention of law enforcement, investigators must obtain search warrants for all devices once they have made an arrest and acted on a search warrant for the offender's home and any other potential storage sites. If the CSAM was reported by or found on a social media site or cloud storage company, a timely preservation request must be filed to ensure both the CSAM and the user's information are not deleted.³² If the CSAM is only held locally on a device, investigators must then find a way to get into the device if the offender is unwilling to provide law enforcement with their passwords.

Several programs are available on the digital forensics market for law enforcement to employ in trying to crack into a password-protected device. GrayKey by GrayShift, for example, allows investigators to connect a locked cell phone to the GrayKey box for a few minutes, after which the phone will reveal its password in anywhere from a few hours to several days.³³ "The exact length of time varies, taking . . . hours . . . [or] up to three days or longer for six-digit passcodes," according to Grayshift.³⁴ After the device is unlocked, the contents of the device can be downloaded to the GrayKey device and analyzed through the GrayKey web-based interface for investigators' review.³⁵ Similarly, Cellebrite's Universal Forensics Extraction Device is marketed to investigators as a tool to help gain entry into devices and pull their data by making full file system copies or creating condensed extraction reports.³⁶ Privacy concerns are always at issue: in constant attempts to ensure users' privacy, technology giants such as Apple continue to try to patch the holes that allow mobile device forensics companies to access users' devices.³⁷

Once the device has been unlocked, whether via a provided password or the use of a forensic tool, investigators must then analyze the data. Digital forensics tools such as Griffey are used to look at large amounts of data, both with the assistance of artificial intelligence and through manual review.³⁸ Griffey advertises its ability to presort or flag certain types of data for users, such as suspected CSAM or terrorism-related material.³⁹ It also includes features that allow for the filtering of mass amounts of data by motion, objects, or selected

32. See Daniel Garric, *Understanding Deleted Files, Unallocated Space, and Their Impact on E-Discovery*, THOMSON REUTERS (Dec. 28, 2017), <https://www.thomsonreuters.com/en-us/posts/legal/understanding-e-discovery/> [<https://perma.cc/E28N-X8ZM>].

33. Thomas Reed, *GrayKey iPhone Unlocker Poses Serious Security Concerns*, MALWAREBYTES (Mar. 15, 2018), <https://www.malwarebytes.com/blog/news/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns> [<https://perma.cc/4DLU-VC33>].

34. *Id.*

35. *Id.*

36. *Cellebrite UFED: The Industry Standard for Lawfully Accessing and Collecting Digital Data*, CELLEBRITE, <https://cellebrite.com/en/ufed/> [<https://perma.cc/UW7Y-T6BL>] (last visited Nov. 12, 2025).

37. Thomas Brewster, *Apple Just Killed The 'GrayKey' iPhone Passcode Hack*, FORBES (Oct. 24, 2018), <https://www.forbes.com/sites/thomasbrewster/2018/10/24/apple-just-killed-the-graykey-iphone-passcode-hack/> [<https://perma.cc/E8NX-QKUN>].

38. *Transform Digital Media Overload into Investigative Insight*, MAGNET FORENSICS, <https://www.magnetforensics.com/products/magnet-griffey/> [<https://perma.cc/MA4C-9CUF>] (last visited Nov. 12, 2025).

39. *Id.*

faces in the pictures and videos.⁴⁰ While all of these features are helpful, ultimately, investigators must put eyes on each and every piece of suspected CSAM to verify that it meets their state's statutory requirements for being classified as CSAM, if it is not an image or video with a hash value already known to NCMEC.

C. *Recovering Deleted Files*

It is unlikely that offenders will delete CSAM files unless they suspect that they are being monitored by law enforcement. The fact that “[CSAM is] likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense[.] Since [CSAM is] illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them.”⁴¹ However, offenders deleting CSAM is not unheard of and presents distinct challenges for investigators.

In some cases, files that have been deleted by the offender can be recovered with the help of forensic tools, as pressing a “delete” button does not simultaneously remove the file from the computer or device.⁴² When a file is deleted, the physical location where the deleted file used to reside is marked by the device as unallocated space, meaning that it appears free when the device is looking for space to save another file.⁴³ The file is not actually removed from the device and irretrievably gone until another file overwrites it and claims the unallocated space.⁴⁴ Until that point, the file is marked for deletion and invisible on the user interface, but not yet overwritten, and still extant in the device's unallocated file space.⁴⁵ Forensic imaging software allows investigators to search and view the contents of the device's unallocated space,⁴⁶ meaning that they can sometimes pull back images that the offender had deleted.

Unallocated space is a pool of storage resources that the system reuses as needed, and cannot intentionally be managed by the device's operator.⁴⁷ Therefore, investigators cannot predict if they will be able to recover deleted CSAM. The overwriting process is random, as the system pulls from the unallocated space when a new file is saved to the device. While valuable data may exist in unallocated space, the full amount of data may be unrecoverable; for example, only portions of an image or video could be recovered, depending on how the system overwrites data and uses the unallocated space moving forward.

40. *Id.*

41. U.S. v. Lamb, 945 F. Supp. 441, 460 (N.D.N.Y. 1996).

42. Joan Feldman, *The Basics of Computer Forensics*, 12 PRAC. LITIG. 17, 19–20 (2001).

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

47. Garrie, *supra* note 32.

D. Preventing Remote Deletion

Throughout the investigatory process, it is critical that no one, investigator or suspect, alters the data on the seized devices. Investigators utilize different techniques to attempt to minimize the potential for remote deletion, ranging from physically isolating the device from Wi-Fi and data networks to engaging built-in features to remove the device from remote access options.

“Isolation of a cellular phone can be accomplished through the use of Faraday bags or radio frequency shielding cloths[,] [H]owever[,] once they’re employed, it is difficult or impossible to work with the phone because [investigators] can’t see through [physical shielding methods] or work with the phone’s keypad.”⁴⁸ Faraday bags are enclosed, sealed bags that prevent mobile devices from accessing data networks or Wi-Fi signals due to the material that the bags are made of, namely layers of various metals.⁴⁹ While excellent for the transportation of mobile devices, physical methods of preventing remote access, such as the use of a Faraday bag, make the next phase of investigation difficult. Faraday tents, rooms, and enclosures exist, but are often cost-prohibitive.⁵⁰

Often, the easiest way to isolate a device from remote connectivity is to place it in airplane mode, which can be accomplished through a couple of clicks or toggling airplane mode on within the device’s menu.⁵¹ Other communication settings, such as Bluetooth, will need to be manually turned off if they are not automatically disabled by activating airplane mode.⁵² Placing the device in airplane mode will prevent data from being overwritten by incoming texts or calls, and, critically, prevent the device from being able to receive a remote wipe command.⁵³ Placing the device in airplane mode rather than turning it off entirely maintains the opportunity to extract data from the device while it is open and gives examiners the possibility of securing an After First Unlock (“AFU”) extraction.⁵⁴ A device that is in the AFU state has been unlocked at least once since the device was reset or completely powered off.⁵⁵ AFU extractions allow

48. Cynthia Murphy, *Developing Process for Mobile Device Forensics*, MOBILE FORENSICS CENT., <https://web.archive.org/web/20140327090806/http://www.mobileforensicscentral.com/mfc/documents/Mobile%20Device%20Forensic%20Process%20v3.0.pdf> [https://perma.cc/S8B8-37QC] (last visited Nov. 12, 2025).

49. *What Is a Faraday Bag?*, DISKLABS, <https://faradaybag.com/what-is-a-faraday-bag/> [https://perma.cc/D9VJ-CT55] (last visited Nov. 12, 2025).

50. Murphy, *supra* note 48.

51. *Id.*

52. *How Should Mobile Devices Be Handled to Prevent Loss of Evidence (Data)?*, VA. DEP’T OF FORENSIC SCI., https://dfs.virginia.gov/question_answer/how-should-mobile-devices-be-packaged-to-prevent-loss-of-evidence-data/ [https://perma.cc/M4CU-4TLZ] (last visited Nov. 12, 2025).

53. *Airplane Mode Forensics—Mobile Device Forensics*, CELLEBRITE, <https://cellebrite.com/en/glossary/airplane-mode-forensics-mobile-device-forensics/> [https://perma.cc/VU4W-SA78] (last visited Nov. 12, 2025).

54. *Id.* The AFU state is one of two states a cell phone can be in, the other being Before First Unlock (“BFU”). A cell phone in the BFU state has been powered off and has not been signed back into using the screen lock passcode. See William Campbell, *BFU and AFU Lock States*, DAKOTA STATE UNIV. (Aug. 23, 2023), <https://blogs.dsu.edu/digforce/2023/08/23/bfu-and-afu-lock-states/> [https://perma.cc/US66-BBRR].

55. Campbell, *supra* note 54.

for the widest capture of data and prevent the device from rebooting after being locked or turned off, which could lead to data loss.⁵⁶

If the device is already powered off when it is seized, it is critical that it remains powered off to prevent the device from connecting to Wi-Fi, Bluetooth, or a cellular data network, and it is recommended that investigators remove the battery or SD card as an additional safety measure.⁵⁷

III. A REVIEW OF STATE FORFEITURE PROVISIONS

Federal prosecutors may move for the forfeiture of CSAM-related equipment under 18 U.S.C. §§ 2253 and 2254, which allow for the forfeiture of physical materials that contain CSAM (presumably including storage drives) as well as materials falling under the catch-all provision inclusive of “any property, real or personal, used or intended to be used to commit or to promote the commission of” CSAM-related offenses.⁵⁸ Not every CSAM case is adopted federally, however, meaning that many state-level prosecutors may handle cases involving thousands of images and devices used to produce, transmit, or store those images. State-level cases often involve law enforcement forces with far less access to funding to investigate these crimes, so state CSAM-related forfeiture provisions are a great tool for combating the small budgets ICAC units are often facing while repurposing offenders’ tools for good.

As of 2025, sixteen states have forfeiture provisions on the books relating to CSAM and crimes of child sexual abuse.⁵⁹ State laws vary greatly in their forfeiture provisions, some facially permitting only very specific items to be forfeited after a seizure by law enforcement, and some allowing for a wide range of forfeitures, so long as the items in question are tied to the commission of the crime or stemming from the proceeds of the crime. This Part displays the results of a nationwide survey of state forfeiture statutes and delves into some state-specific forfeiture provisions designed to address the fate of the devices used to create, store, and disseminate CSAM.

A. Alabama

Alabama’s CSAM-related forfeiture provision is rather broad, declaring that, “[a]ny article, equipment, machine, materials, matter, vehicle, or other thing used in the commercial production, transportation, dissemination, display, or storage of any child sexual abuse material shall be contraband and shall be

56. *Airplane Mode Forensics—Mobile Device Forensics*, *supra* note 53.

57. *How Should Mobile Devices Be Handled to Prevent Loss of Evidence (Data)?*, *supra* note 52.

58. 18 U.S.C. § 2253(A)(1–3). *See also* 18 U.S.C. § 2254 (detailing the process for forfeiture).

59. State statutes discussed in this Part will be cited within the corresponding Section. The states not discussed below are Alaska, Georgia, Maine, Maryland, Nevada, South Dakota, Texas, and Wyoming. *See* ALASKA STAT. § 11.61.129(a); O.C.G.A. § 16-12-100; 17-A ME. REV. STAT. § 285(1); MD. CRIM. L. CODE § 11-211 (2024); NEV. REV. STAT. 200.760; S.D. REV. STAT. 22-24A-15; TEX. PEN. CODE 59.01(2)(A)(iii); WY. REV. STAT. 6-4-303(f)(iii).

forfeited to the State of Alabama.”⁶⁰ As equipment used in the storage of CSAM, high-volume external storage drives certainly qualify for forfeiture. There is no further instruction on what law enforcement is then required to do with the forfeited items, so repurposing them as investigatory storage tools is a viable option.

Curiously, the mechanics of the forfeiture itself are comparable to those employed to forfeit items used in the illegal transportation of alcoholic beverages.⁶¹ This may be attributable to the fact that, in many cases, CSAM-related offenses are listed with other crimes against morality or the public good in state statutes.

B. Arizona

Arizona’s CSAM-related forfeiture provision does not require any type of notice or hearing before the involved items are forfeited to the state, instead proscribing that upon conviction of a CSAM-related offense, “the court **shall order** that any photographic equipment, computer system or instrument of communication that is owned or used exclusively by the person and that was used in the commission of the offense be forfeited.”⁶² This forfeiture provision then gives law enforcement three options in regards to what can happen to the forfeited equipment: it can be sold, destroyed, or “otherwise properly disposed.”⁶³

Although not explicitly included, there is an argument to be made that external storage drives are a part of the computer system used by the offender, and thus, are subject to forfeiture to law enforcement. Repurposing the drives for use in further investigations seems to qualify as another form of proper disposal, so long as they are wiped clean of the original material that was brought to investigators’ attention and kept securely in the possession of the investigating agency.

C. California

California’s CSAM-specific forfeiture provision is unique in that it does not require a criminal conviction to be secured prior to the forfeiture and destruction of items used in producing, disseminating, or storing CSAM.⁶⁴ Instead, if moved to do so, the court may enter an order for the destruction of such material and the devices used to create, disseminate, or store it, independent of the criminal case’s timetable.⁶⁵ This is notable in two respects. First, no

60. ALA. CODE § 13A-12-198 (2024).

61. “The manner, method, and procedure for the forfeiture and condemnation of the thing shall be the same as is provided by law for the confiscation, condemnation, or forfeiture of automobiles, conveyances, or vehicles in which alcoholic beverages are illegally transported.” *Id.*

62. ARIZ. STAT. § 13.3557 (emphasis added).

63. *Id.*

64. CAL. PEN. CODE 312(f).

65. *Id.*

conviction is required to forfeit the items to the state and have them destroyed by law enforcement. In practice, this may result in the loss of evidence in a pending case if an overzealous prosecutor or law enforcement officer moves for an order of forfeiture and destruction. However, if the perpetrator dies or flees the area and there is no hope of a criminal prosecution on the horizon, this provision prevents the devices from ever falling into the wrong hands and the material from making its way further out into the world. Additionally, if there is a legal issue that prevents the case from being prosecuted, such as a faulty search warrant, the lack of a requirement for conviction before forfeiture means that the devices will not be released back to the offender, priming them for continuing to offend.

Secondly, this provision is notable because it leaves law enforcement with no option but to destroy the forfeited items. While states such as Arizona specify that destruction of the devices is not the only avenue law enforcement can pursue, California law seems to put investigators in a bind by requiring that they destroy what could be a useful investigatory tool.

D. Illinois

Illinois' CSAM-related forfeiture provision encompasses not only CSAM but also depictions of "a person with a severe or profound intellectual disability engaged in any activity described in" the list of sexual acts laid out within its definition of CSAM.⁶⁶ Illinois is the only state with a CSAM-related forfeiture provision to include another vulnerable population in its forfeiture law. However, the reasoning behind it is sound: both populations are especially vulnerable victims, and most likely have limited control over what happens to the material once it is created.

This forfeiture provision is sweeping, including not only physical copies of CSAM (such as films, videotapes, photographs, or their digital equivalents) but also "any material or equipment used or intended for use in photographing, filming, printing, producing, reproducing, manufacturing, projecting, exhibiting, depiction by computer, or disseminating such material."⁶⁷ External storage drives assist in the projection (on a monitor), exhibition (again, on a monitor), and computer depiction of CSAM, and thus fall within the forfeiture law. Illinois does not mandate the destruction of the devices once forfeited, so wiping them and repurposing them for law enforcement use is permissible.

E. Nebraska

Nebraska law specifies that the forfeiture of CSAM-related devices can be part of the sentence imposed on the offender if the court, in a separate hearing within the same prosecution, finds by clear and convincing evidence that the device was used or intended to be used to facilitate the production, dissemination,

66. 720 ILL. COM. STAT 5/11-20.1(e).

67. *Id.*

or possession of CSAM.⁶⁸ Further, this forfeiture is not strictly limited to computers and related electronic devices: “a sentencing court may order that any money, securities, negotiable instruments, firearms, conveyances, or electronic communication devices as defined in section 28-833 or any equipment, components, peripherals, software, hardware, or accessories related to electronic communication devices” are to be forfeited to the state.⁶⁹

While Nebraska law is unclear on what must happen to these devices once they are forfeited, it is clear that external hard drives are included in the array of items that can be forfeited to the state at the end of a CSAM prosecution.

F. Virginia

Virginia law allows for the forfeiture of “[a]ll audio and visual equipment, electronic equipment, devices and other personal property used in connection with the possession, production, distribution, publication, sale, possession with intent to distribute or making of child pornography” or that which is connected to the solicitation of a child for attempted or completed sexual offenses.⁷⁰ The notice and hearing procedure is the same as that which is used in drug, vehicle, and cash asset forfeiture cases.⁷¹ The forfeiture law does not provide a mandate for destruction, leaving law enforcement freely able to repurpose forfeited devices for investigatory purposes.

G. West Virginia

West Virginia’s CSAM-related forfeiture provision lists three categories of forfeiture-eligible materials: (1) the CSAM itself, no matter the form it takes, (2) “[a]ll raw materials, products and equipment of any kind which are used, or intended for use, in manufacturing, processing, delivering, importing or exporting any visual depictions or any crimes against children,” and (3) “[a]ll books, records, research products and materials, including hard drives, microfilm, tapes and data which are used, or have been used, or are intended for use” in producing, disseminating, or possessing CSAM.⁷² Hard drives being specifically named makes a solid case for their forfeiture, and as the statute is silent on any specifically mandated method of disposal, law enforcement agencies are free to wipe the drives and use them for investigatory purposes.

IV. STATE LAW ENFORCEMENT AGENCY POLICIES REGARDING CSAM-RELATED FORFEITURES

Among the states that have CSAM-specific forfeiture provisions on the books, many of their largest cities and counties do not have forfeiture policies on

68. NEB. REV. STAT. 28-813.01(5).

69. *Id.*

70. VA. CODE § 19.2-386.31. See list of offenses cataloged in VA. CODE § 18.2-374.3.

71. VA. CODE § 19.2-386.31.

72. W. VA. CODE § 61-8C-7(a).

file at their police or sheriff's departments. Of those that do have forfeiture policies written into their law enforcement policy manuals, the vast majority only address forfeitures in narcotics cases or similar situations involving cash, vehicles, or weapons. Even in cities that do not restrict forfeitures to drug-related activity, the forfeiture is often managed by the Vice and Narcotics Division. In Houston, Texas, for example, the Houston Police Department's general order on forfeitures indicates that most forfeitures processed by the department must go through the Narcotics Division's Asset Forfeiture Unit in some form, whether the unit is just receiving notice of the planned forfeiture by another unit or is actively participating in the seizure of materials to be forfeited.⁷³

The Houston Police Department placed an additional hurdle for ICAC investigators in its policy by requiring that all non-contraband items seized aside from cash, vehicles, boats, or aircraft have a total sale value of \$5,000 or greater.⁷⁴ The value of individual external storage drives varies greatly, and many lower-level CSAM cases may not involve \$5,000 worth of otherwise forfeiture-eligible devices, meaning that investigators will miss out on the benefit of the use of such drives in future cases. The general order does, however, allow for exceptions to the standard requirements if the assistant chief of the appropriate investigative division and the Narcotics Division's assistant chief agree to waive the normal requirements.⁷⁵

In Harris County, Texas (which encompasses the city of Houston), the sheriff's department imposes a similar \$2,000 minimum threshold value for forfeited materials, with some exceptions.⁷⁶ CSAM case-related electronic equipment is not one of the listed exceptions, meaning that while the threshold for seizure is lower than in the local police department, if the \$2,000 value is not reached, the equipment will likely be destroyed as containing contraband instead of forfeited.

The Virginia Beach, Virginia, Police Department has a \$350 minimum value requirement for a single forfeiture-eligible item, but states that, because each case is different, the guidelines are flexible and the Commonwealth's Attorney's Office can approve a forfeiture that does not meet the \$350 minimum value.⁷⁷ This forfeiture review provision allows investigators and prosecutors to work together to broaden the range of investigative tools at law enforcement's disposal. Additionally, the much lower value threshold allows for the forfeiture

73. *General Order 700-08: Asset Seizure and Forfeiture*, HOU. POLICE DEP'T (Oct. 20, 2021), https://www.houstontx.gov/police/general_orders/700/700-08%20Asset%20Seizure%20and%20Forfeiture.pdf [<https://perma.cc/JSK7-CXTC>].

74. *Id.* at 700-08(1)(1)(2).

75. *Id.* at 700-08(4).

76. 613—*Asset Seizure, Forfeiture, and Disposition of Contraband Property*, HARRIS CNTY. SHERIFF'S DEP'T, <https://hcsopolicy.com/policy/613-asset-seizure-forfeiture-and-disposition-of-contraband-property/> [<https://perma.cc/4Y4G-Q844>] (last visited Nov. 12, 2025).

77. *General Order 16.02: Asset Forfeiture*, VA. BEACH POLICE DEP'T (Aug. 2024), <https://s3.us-east-1.amazonaws.com/virginia-beach-departments-docs/police/Your-VBPD/Policies-and-Field-Guides/Policies/16.02-Asset-Forfeiture.pdf>.

and repurposing of devices that may be valuable sources of storage but not extremely valuable on the resale market.

Despite having CSAM-specific forfeiture laws on the books, very few major cities in the sixteen states with such laws have police or sheriff's department policies that address these types of forfeitures, even indirectly. Even fewer seem to employ them: a quick search for CSAM-related forfeiture cases yields negligible results in the news, at least on the state level. Investigators in states with such laws should be taking advantage of them in order to gain access to investigatory tools they can use to further future ICAC investigations without having to utilize their own funds or forego bringing cases that their administrations cannot feasibly pay to investigate.

V. CONCLUSION

Although a third of states have extant CSAM-specific forfeiture laws, they are generally underutilized. Those that do have laws on the books differ greatly in their listed devices (though a catch-all provision is usually added) and requirements for destruction of forfeited devices.

In constructing a CSAM-specific forfeiture law, legislators should permit a wide range of forfeiture-eligible materials, including but not limited to any computer equipment or external storage drives used in the creation, possession, or distribution of CSAM. It is critical to catch all potential avenues for storage, be it storage on the hard drive of the computer or device, or an external device that can be removed and swapped out for additional storage. A wide-ranging list of material eligible for forfeiture provides investigators with the greatest potential of tools to repurpose for future use in new cases. It also removes the greatest number of potential devices from convicted offenders, making it more difficult for them to reoffend. As with any other type of forfeiture, however, the nexus to the crime must always be shown to prevent any overreach by the investigating agency or the prosecuting attorney's office.

Secondly, in order to allow for the repurposing of drives for further investigatory use, such statutes should not require their destruction. While it is important that the CSAM itself be destroyed, local law enforcement should be given the statutory option to either destroy forfeited drives or repurpose them once the CSAM has been removed completely and the drive has been returned to its factory settings. Mandatory destruction on its face seems to be a positive thing, but it forestalls the possibility of using the storage space for good.

As for local law enforcement policies, having no dollar amount threshold for forfeiture of CSAM-related equipment would greatly help investigators, as external storage drives vary widely in price depending on the brand and amount of storage available. Even an aggregate amount threshold could cause issues in lower-level cases where an offender has vast amounts of storage, but the total value of the devices remains less than the department's required dollar amount. If an agency needs to impose a value threshold, there should always be a method to petition for an exception, be it solely accomplished through the approval from

the chain of command or in conjunction with the local prosecutor who is tasked with handling forfeiture cases.

In states with no statutorily proscribed method for forfeiting CSAM-related storage drives, law enforcement policies should encourage following the state's standard forfeiture procedure in order to procure a court order allowing for the drives' reuse in investigations or training.⁷⁸ While following this process will likely require the aid of the local prosecutor's office, this method gives law enforcement the assurance of a court's approval, which is critical when handling such sensitive items.

CSAM-specific forfeiture provisions in state law are valuable tools for investigators facing low budgets for equipment. Local police and sheriff's departments would benefit greatly from adopting policies that promote the repurposing of CSAM-related computer equipment as investigatory tools. The use of these hidden statutory gems, along with department policies that permit wiping and reusing these devices for good, has the potential for expanding underfunded ICAC units' abilities to combat online child exploitation, which is very clearly on the rise. In 2013, NCMEC received an average of 1,380 CSAM-related tips per day.⁷⁹ By 2023, NCMEC was receiving over 100 thousand tips each day.⁸⁰ In total, NCMEC received 35,925,098 CyberTipline reports regarding the creation, possession, and distribution of CSAM in 2023 alone.⁸¹ By taking advantage of underutilized statutory tools, investigators could have a great impact on these numbers and on the lives of the children who are being exploited to create CSAM worldwide.

78. Thanks to Det. Brandon Styers, Mooresville Police Department, Mooresville, NC, for sharing local policy and suggestions from a state that does not have a CSAM-specific forfeiture law.

79. Chuck Grassley, *Q&A: Protecting Kids Online*, MEDIUM (Feb. 2, 2024), <https://medium.com/@ChuckGrassley/q-a-protecting-kids-online-028cefc11f1b> [<https://perma.cc/7JRG-L9RX>].

80. *Id.*

81. NAT'L CTR. FOR MISSING & EXPLOITED CHILD., CY 2023 REPORT TO THE COMMITTEES ON APPROPRIATIONS (2024), <https://le.utah.gov/interim/2024/pdf/00003099.pdf> [<https://perma.cc/3PSU-LYKK>].