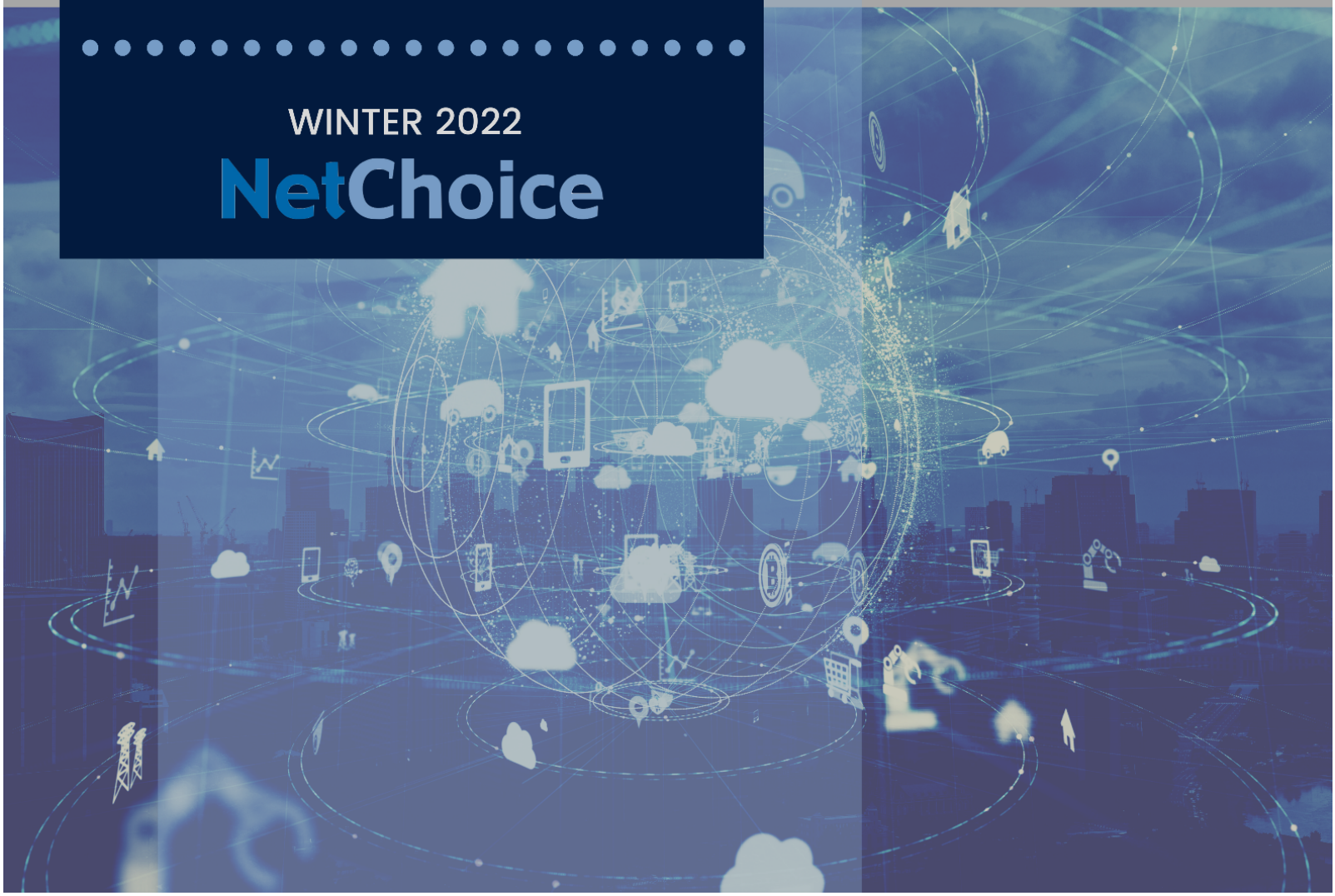
THE EARN IT ACT OF 2022 COULD ACTUALLY HELP CHILD ABUSERS ESCAPE JUSTICE. THE ACT RISKS FOURTH AMENDMENT IMPLICATIONS THAT COULD LET DEFENDANTS WALK FREE WHILE THE THIRD-PARTY DOCTRINE OFFERS LITTLE HELP.

THE EARN IT ACT OF 2022 HAS CRITICAL FOURTH AMENDMENT ISSUES

WINTER 2022

NetChoice



Fourth Amendment Concerns

The EARN IT would lead to bad outcomes in many criminal cases involving charges of CSAM. That is because EARN IT jeopardizes the delicate constitutional balance that currently exists by enshrining the government's preference that private parties search for and report suspected instances of CSAM. Under the exclusionary rule, some of this evidence may be at risk of exclusion.

The Fourth Amendment and its warrant requirement apply only to government actors. But when private actors search or seize because of the government's "encouragement"—in whole or in part—the Fourth Amendment applies to them as well. *Skinner v. Railway Lab. Execs. Ass'n*, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government.").

Even when the law does not directly compel private parties to search or seize evidence, courts consider "all the circumstances of the case" **to determine whether "the Government did more than adopt a passive position toward the underlying private conduct.**" *Id.* at 615-16. In other words, "that the Government has not compelled a private party to perform a search does not, by itself, establish that a search is a private one." *Id.* at 615. In fact, **when the government makes plain its "strong preference" for private searches, or "its desire to share the fruits of such intrusions," the Fourth Amendment applies**. *Id.* at 615-16.

To understand EARN IT's potential to violate the Fourth Amendment, consider the parallels between EARN IT and *Skinner*:

Skinner	**EARN IT**
• Congress's decision to *allow*—but not require—railroads to conduct blood and alcohol tests of their employees by removing roadblocks (including state laws and employment contracts) signaled the government's desire for private parties to conduct such searches.	• Congress's decision to *allow*—but not require—states to enforce their own CSAM laws (including laws that explicitly require or encourage searching) signals Congress's desire for private parties to search for CSAM. • Congress's decision to establish a commission to develop best practices, including ones related to evidence retention and reporting to law enforcement, signals the government's preference that such searches occur *and* the government's desire to share in the fruits of those searches.

Please see NetChoice's full report on EARN IT's Fourth Amendment problems (available here).

Federal Case Law Makes Clear that Private Searches Must be Completely Voluntary to Escape the Fourth Amendment.

Eight years before the U.S. Supreme Court decided *Skinner*, the U.S. Court of Appeals for the Ninth Circuit decided a case that established what has become a widely cited test for determining when a private search becomes a governmental search. *United States v. Walther*, 652 F.2d 788 (9th Cir. 1981). The test was established in the context of a search of luggage by an airline employee. When the airline employee found drugs in a piece of luggage, he notified the federal Drug Enforcement Administration. The DEA had no prior knowledge of this search, nor did it provide him any reward. Nonetheless, the fact that the DEA in the past had provided rewards to this employee, who had previously worked as a confidential informant for them was enough for the court to conclude that the airline employee was an "instrument or agent" of the government. *Id.* at 792. As a result, the airline's search was subject to Fourth Amendment standards—and the drug smuggler who had shipped cocaine in her airline luggage was able to exclude the evidence from her criminal trial. *Id.* at 791.

The test enunciated in this case, *United States v. Walther*, has been followed across most of the other U.S. circuit courts, including in the context of searches by internet companies. Jeff Kosseff, *Private Computer Searches and the Fourth Amendment*, 14 I/S A J. of L. & Pol'y for the Info. Society 187, 198 (2018). It asks two questions:

(1) What was the level of the government's knowledge and acquiescence in the search?
(2) What was the intent of the party performing the search? *Walther*, 652 F.2d at 792.

In *Walther*, the court applied the first prong of this test in a way that made it well-nigh impossible for the federal government to argue that the Fourth Amendment was not implicated. Whereas the government claimed, with 100% accuracy, that it knew nothing about the search before it had already taken place, the court found that the government could nonetheless be said to have acquiesced in the airline employee's search because it had "encouraged" the employee to engage in this type of search in the past, had "rewarded" him for providing drug-related information before, and had known of his pattern of search history and had not discouraged it. Thus, the government was "involved" in this search—not as a participant, but "indirectly as an encourager of the private citizen's actions." *Id.* at 791. There need not be "overt governmental participation"; instead, there must only be more than "the complete absence of such participation." *Id.*

The court's application of the second part of the test similarly made application of the Fourth Amendment unavoidable. Acknowledging that the facts of the case fell within a "gray area," the court found that the airline employee acted because he was suspicious that the luggage contained illegal drugs. *Id.* This, it decided, was tantamount to his serving as an agent of the government, because the government itself was concerned with illegal drugs. *Id.* at 792. All this supported a finding that the employee was fulfilling a governmental objective and might have been motivated by the possibility of a DEA reward—even though he did not get one, and apparently did not even seek one. *Id.* at 791-92.

On the basis of this unlikely legal template, seemingly so hostile to the notion of keeping private searches free from Fourth Amendment strictures, the lower federal courts have constructed a body of case law that is actually quite favorable to the notion of internet platforms conducting private searches that do not risk subsequent application of the Exclusionary Rule. Under the *Walther* test, as well as the more recent U.S. Supreme Court precedent in *Skinner*, the government has successfully prevailed in

arguing that when private internet companies have independent reasons to conduct searches for child sexual abuse material, those companies are not acting as government agents. A brief review of the leading precedents is helpful in understanding why those precedents exist, and why they are not so elastic as to fit what the EARN IT bill has in mind.

Nearly two decades after *Walther*, and applying its principles in the internet context, the Fourth Circuit in 2010 ruled that when America Online produced to NCMEC "the result of routine scanning the company conducts to recognize files that may be detrimental to AOL," it was not acting as a government agent. *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010). Key to the court's determination was the fact that the statutory scheme under which AOL produced the data for NCMEC did not "remotely suggest a congressional preference for monitoring." *Id.* at 366-67. The court contrasted this with *Skinner*, where the explicit authorization for testing indicated a "strong preference for testing." *Id.* at 367.

Two years later, the First Circuit similarly found that when Yahoo! uncovered child sexual abuse material and turned it over to NCMEC, the Fourth Amendment was not implicated because there was "no evidence" that "Yahoo! did what it did to further the government's interest." *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012).

In the 2013 case of *United States v. Stevenson*, the Eighth Circuit considered whether AOL's private search for and production of child sexual abuse material to NCMEC should be subjected to Fourth Amendment constraints, in light of the *Skinner* doctrine that government encouragement can render a private search governmental. 727 F.3d 826 (8th Cir. 2013). The court held that AOL was not acting as a federal agent, reasoning that unlike the regulatory preference for searches betrayed by the federal regulatory permission for drug and alcohol testing in *Skinner*, federal law requiring reporting to NCMEC neither "authorizes AOL to scan its users' e-mails," nor "clears the 'legal barriers' to scanning." *Id.* at 830. Furthermore, federal law was "silent regarding whether or how AOL should scan its users' e-mail." 727 F.3d 826 (8th Cir. 2013).

Five years ago, a federal district court in the Sixth Circuit reached a similar Fourth Amendment result on similar grounds. *United States v. Miller*, No. CV 16-47-DLB-CJS, 2017 WL 2705963 (E.D. Ky. June 23, 2017). In *United States v. Miller*, the issue was whether Google's voluntary scans of emails for child sexual abuse material were in reality the result of "government pressure." *Id.* at *3. The court's decision turned primarily on its analysis of the operative federal law under which Google reported the results of these scans. The court noted that federal law neither authorizes scanning, nor provides a basis for inferring that Google's scanning is primarily motivated to help police investigations. *Id.* at *3-*4.

The same year, a federal district court in the Tenth Circuit ruled that Sony's private searches of PlayStation 3 gaming devices and its reporting of child sexual abuse material to NCMEC did not render it a government agent subject to Fourth Amendment constraints. *United States v. Stratton*, 229 F.Supp.3d 1230 (2017). As in previous cases, the court looked to the federal law under which Sony reported, to determine whether the search was truly voluntary on Sony's part. The court noted that federal law "only requires Sony to file a report if it learns of facts that suggest an incident of child abuse … Sony [need not] act affirmatively to monitor its users' accounts, review its users' downloads, or maintain any sort of reporting system for abuse." *Id.* at 1237.

Finally, in *United States v. Wolfenbarger*, decided last year, a federal district court in the Ninth Circuit determined that Yahoo! did not act as a government agent when it searched for child sexual abuse

material and turned it over to NCMEC, because its decision to screen emails was voluntarily made for business reasons. No. 16-CR-00519-LHK-1, 2019 WL 6716357 (N.D. Cal. Dec. 10, 2019). Once again, the bedrock of that conclusion was the lack of inducement in federal law that might indicate government encouragement was part of the motivation. "Most importantly," the court said in concluding its analysis, federal law "imposed no duty on Yahoo to monitor its platform for child exploitation materials." *Id.* at *10.

The pattern established in these cases is clear to see. Courts have been willing to permit private internet platforms to conduct searches of third-party data, and to turn it over to NCMEC by law, without incurring Fourth Amendment penalties because in each case they have judged that the internet platform is acting for its own private, commercial purposes. In each case they have underscored their reliance on the fact that existing federal law lacks material inducements for private searches, meaning that the element of government encouragement is missing.

EARN IT's combination of encouragement, endorsement, penalties, and explicit guidance unmasks the government's "strong preference" for searches. The result is that a search that might have been deemed private, but for the EARN IT bill, could now be subject to the Fourth Amendment and the Exclusionary Rule because under the applicable Supreme Court precedent of *Skinner*, it cannot be said to be primarily the company's own initiative.

There is a tragic irony in this. Currently, internet companies including Google, Facebook, and Twitter need not worry that the data they turn over to NCMEC will be excluded from evidence in a criminal trial because a court might later determine they were acting as an agent of the government in conducting their searches. This is so because the government has been able to claim that it does not have "any role in instigating" searches for child sexual abuse material. The EARN IT bill, however, not only encourages searches for CSAM, but in some cases requires them—vis-a-vis state law. screening. This would have the unintended effects of both frustrating the government's criminal prosecutions and undermining the companies' genuine self-interest in keeping their platforms free from child-exploitation material.

The Third-Party Doctrine Likely Offers Little Help

EARN IT's supporters have claimed that even if the bill violates the Fourth Amendment, evidence seized under it may still be admissible in criminal trials under exceptions to the warrant requirement. In particular, advocates have pointed to the "third-party doctrine" exception to the Fourth Amendment. While this exception is admittedly broad, it is not so broad as to sanction screening of all private communications and content stored on devices or in the cloud. To the contrary, the Supreme Court has clarified that the doctrine should not be automatically extended to digital data.

Only four years ago, in *Carpenter v. United States*, the Supreme Court held that the government's review of location data from an individual's cell phone use constitutes a search for Fourth Amendment purposes. This is so even though the information the government obtained consisted solely of business records that were compiled by a private company, with the consent of the individual. Even though the data were not compiled for the purpose of aiding a government search, the Fourth Amendment applied once the government attempted to use the data in a criminal trial. 138 S. Ct. 2206, 2217-21 (2018).

Carpenter represented a sea change in the Court's third-party doctrine. As Justices Gorsuch, Thomas, and Alito pointed out in their dissents, the majority opinion carved an exception to the third-party doctrine exception: When the government seeks sensitive information about an individual and that

information flows from the individual's data, the government must now seek a warrant. To be sure, the majority opinion explicitly limits *Carpenter*'s holding to historic location data, but as the dissents all persuasively argue, the rationale behind *Carpenter* easily extends to most forms of data generated through devices and digital services.

Consider that the Fourth Amendment "seeks to secure 'the privacies of life' against 'arbitrary power.'" *Carpenter*, 138 S. Ct. at 2213-2214 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). So when "the government violates a subjective expectation of privacy that society recognizes as reasonable," it also violates the Fourth Amendment. *Kyllo v. United States*, 533 U.S. 27, 33 (2001); see *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Although "no single rubric definitively resolves which expectations of privacy are entitled to protection," *Carpenter*, 138 S. Ct. at 2213, intimate information that the government collects through new technology retains Fourth Amendment protection, even when someone shares that information with a third party. *See id.* at 2217-19. That's because an individual has a greater expectation of privacy in information—regardless of source—that "provides an intimate window into [her] life." *Carpenter*, 138 S. Ct. at 2217 (citing *Jones v. United States*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

In other words, expectations of privacy—even under the third-party doctrine—operate on a sliding scale. *Compare Kyllo*, 533 U.S. at 37 ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.") (emphasis in original) *with California v. Greenwood*, 486 U.S. 35, 40 (1988) (holding there is no reasonable expectation of privacy in "plastic bags left on or at the side of a public street [that] are readily accessible to animals, children, scavengers, snoops, and other members of the public"). So even though "an individual has a reduced expectation of privacy in information knowingly shared with another," that "'does not mean that the Fourth Amendment falls out of the picture entirely.'" *Carpenter*, 138 S. Ct. at 2219 (quoting *Riley v. California*, 134 S. Ct. 2473, 2488 (2014)).

And when "'the nature of the particular documents sought'" is unlike the "limited types of personal information addressed in Smith and Miller," the Fourth Amendment still applies. *Id.* (quoting *Miller*, 425 U.S. at 442) (internal quotations omitted). In *Smith*, the Court found that "telephone call logs reveal little in the way of 'identifying information,'" *Carpenter*, 138 S. Ct. at 2219 (quoting *Smith*, 442 U.S. at 742), and in *Miller*, the Court found that checks are "not confidential communications but negotiable instruments to be used in commercial transactions" and thus the Bank Secrecy Act of 1970, which authorized warrantless screening of bank transactions, was constitutional under the Fourth Amendment. 425 U.S. at 442.

The third-party doctrine is unlikely to save EARN IT from Fourth Amendment scrutiny. To be sure, the Fourth Amendment's application will depend in part on the specific facts of each case. For example, one could readily imagine a court holding that there is no Fourth Amendment violation when a platform finds and reports CSAM that was shared publicly on the platform. By contrast, it is entirely likely that *at least some courts* will find a Fourth Amendment violation when the screening, searching, or filtering encompasses private communications between users.

At bottom, digital data is not like checks deposited in a bank account. A check must identify the parties and amounts involved—and because the individual depositor understands that this information *must* be communicated to the bank for the transaction to work—there is a reduced expectation of privacy. And like a letter sent in the mail, these "external" indicia are necessary components of completing the underlying act: the sender is directing a third party to do something based on that public information. But just as the Post Office may not open sealed letters and read their contents without violating the

Fourth Amendment, neither may the government read information sent in ostensibly private communications without implicating the warrant requirement.

Technology & Fourth Amendment Originalism

As Justice Scalia explained in *Kyllo* and Chief Justice Roberts affirmed in *Carpenter*, when science and technology—and the digital products they generate—"enhance[] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, at 2214 (2018) (quoting *Kyllo*, 533 U.S. at 34 (2001)). Instead of using a "mechanical interpretation" of the Fourth Amendment and leaving expectations of privacy "at the mercy of advancing technology," the Supreme Court stops the government from exploiting new technology. *Kyllo*, 533 U.S. at 35. And because the Fourth Amendment safeguards privacy, "[w]hether the Government employs its [own] technology" or "leverages the technology" from another source, the information targeted is still protected. *Carpenter*, 138 S. Ct. at 2217.

What is more: any government attempt to distinguish between use of new technology to generate a record for investigative purposes, as in *Kyllo*, and use of records already created by new technology for non-investigative purposes, will likely fail. Even when "records are generated for commercial purposes," "that distinction does not negate [an] anticipation of privacy." *Carpenter*, 138 S. Ct. at 2217. **What matters is the government's ability to collect a new category of information because of new technology**. *Id*. And here, there can be no doubt that digital services like social media platforms have created broad new categories of information that, but for such technology, the government would need a warrant to obtain.

Encryption Concerns

Although the bill now includes Senator Leahy's encryption amendment, it still leaves Americans and their data vulnerable to bad actors, including foreign governments.

The original Leahy amendment attempted to avoid triggering the Fourth Amendment by stating that companies could not be held liable for their use of encryption or for offering to users the choice to use encryption, their inability to decrypt messages, or their refusal to build backdoors into their products. The new version of EARN IT replaces the Leahy Amendment with language from the 2020 House version of the bill and specifically says that companies' use of encryption could still be considered a factor in determining whether they are liable.

In section 5 of the bill, 7(A) delineates instances of encryption that cannot be used against a covered entity in court. In the same section, 7(B) backtracks on that safe harbor. In this case, the exception swallows the rule. Language that was initially written to ensure that encryption is not criminalized turns around and criminalizes encryption in particular instances - a distinction without a difference.

Americans all over the world depend on encryption to keep their private correspondence and information safe. Requiring or threatening companies to weaken encryption services leaves our data vulnerable to breaches. Diminishing American access to encryption makes us easier targets for criminals, foreign adversaries, and rogue regimes.