United States Court of Appeals
For the Second Circuit

August Term 2024

Submitted: October 16, 2024
Decided: September 10, 2025

No. 23-6886

UNITED STATES OF AMERICA,

Appellee,

v.

WESLEY GUARD,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of New York
No. 1:22CR00105,
Mae A. D'Agostino, *Judge*.

Before: JACOBS, MERRIAM, *Circuit Judges*, and VILARDO, *District Judge*[*].

[*] Judge Lawrence J. Vilardo of the Western District of New York, sitting by designation.

Defendant-appellant Wesley Guard appeals from a judgment entered in the United States District Court for the Northern District of New York (D'Agostino, *J.*), convicting him, following a jury trial, of transportation, receipt, and possession of child pornography in violation of 18 U.S.C. §2252A. Guard contends that the District Court erred in denying his pretrial motion to suppress evidence obtained in, or that was the fruit of, searches conducted by Kik, a mobile chat messaging application and electronic service provider. He argues that Kik acted as an agent or instrument of the National Center for Missing and Exploited Children ("NCMEC") when it reviewed his accounts for child sexual abuse material and that NCMEC is a governmental entity for purposes of the Fourth Amendment.

We conclude that NCMEC is a governmental entity. However, Guard failed to meet the burden, on this record, of showing that Kik's review of his electronic accounts and data triggered the protections of the Fourth Amendment.

Guard makes a number of other challenges to his convictions and sentence, most of which we find unpersuasive. We agree with Guard that the written judgment does not conform to the District Court's oral pronouncement of certain discretionary conditions of supervised release. Accordingly, we **AFFIRM IN PART**, and **VACATE and REMAND IN PART**, with instructions to amend the written judgment to conform with the oral pronouncement of Special Conditions 2, 4, and 7.

James P. Egan, Assistant Federal Public Defender, Office of the Federal Public Defender, Syracuse, NY, *for Defendant-Appellant*.

Joshua Rothenberg, Adrian LaRochelle, *for* Carla B. Freedman, United States Attorney for the Northern District of New York, Syracuse, NY, *for Appellee*.

SARAH A. L. MERRIAM, *Circuit Judge*:

Defendant-appellant Wesley Guard appeals from a judgment entered in the United States District Court for the Northern District of New York (D'Agostino, *J.*), convicting him, following a jury trial, of transportation of child pornography, in violation of 18 U.S.C. §2252A(a)(1) and (b)(1); receipt of child pornography, in violation of §2252A(a)(2)(A) and (b)(1); and possession of child pornography, in violation of §2252A(a)(5)(B) and (b)(2). Guard was sentenced principally to 151 months of imprisonment and 15 years of supervised release.

On appeal, Guard contends that the District Court erred in denying his pretrial motion to suppress evidence obtained in, or that was the fruit of, searches conducted by Kik, a mobile chat messaging application and electronic service provider. He argues that Kik acted as an agent or instrument of the National Center for Missing and Exploited Children ("NCMEC") when it reviewed his accounts for child sexual abuse material ("CSAM") and that NCMEC is a governmental entity for purposes of the Fourth Amendment.

Guard bears the burden of showing that Kik's review of his electronic accounts and data triggered the protections of the Fourth Amendment. We conclude that he failed to meet that burden. The record before us does not

establish that Kik acted as a governmental agent or instrument when it viewed the contents of Guard's accounts and reported its findings to NCMEC.

Guard makes a number of other challenges to his convictions and sentence, most of which we find unpersuasive. We agree with Guard that the written judgment does not conform to the District Court's oral pronouncement of certain discretionary conditions of supervised release. Accordingly, we **AFFIRM IN PART**, and **VACATE and REMAND IN PART**, with instructions to amend the written judgment to conform with the oral pronouncement of Special Conditions 2, 4, and 7.

BACKGROUND

We begin with an overview of the record evidence regarding Kik, the mobile application by which Guard was found to have possessed, received, and transported CSAM, and how Kik provides information about suspected CSAM to NCMEC. We then turn to the record evidence regarding the search of Guard's Kik accounts.

I. Kik's Operations and Reporting of CSAM to NCMEC Generally

Kik is a messaging application available for download on most mobile phones. It "allows users to chat with one another one-on-one or in a group

setting, [either in a] private or public group." App'x at 315. It also allows users to share images and videos. *See* App'x at 316.

NCMEC "is an entity organized as a private nonprofit but established by Congress and statutorily obliged to operate the official national clearinghouse for information about missing and exploited children." *United States v. Maher*, 120 F.4th 297, 302 n.5 (2d Cir. 2024) (citations and quotation marks omitted); *see also* 34 U.S.C. §11293(b)(1)(B). As part of its statutory mandate, NCMEC "work[s] with families, law enforcement agencies, electronic service providers, . . . technology companies, . . . and others . . . to reduce the existence and distribution of online images and videos of sexually exploited children." 34 U.S.C. §11293(b)(1)(K). It operates a "CyberTipline" that invites members of the public and electronic service providers ("ESPs") to report online child pornography.[2] *See* App'x at 67-68, 284.

Kik uses a software program developed by Microsoft "to identify known

[2] Child pornography "consists of sexually explicit visual portrayals that feature children." *United States v. Williams*, 553 U.S. 285, 288 (2008); *see also* 18 U.S.C. §2256(8)(A) (defining "child pornography" as a visual depiction of sexually explicit conduct where "the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct"). We employ "CSAM" to mean the same and use the terms interchangeably.

images of child pornography that may come across [its] servers through user accounts." App'x at 70; *see also* Hany Farid, *Reining In Online Abuses*, 19 Tech. & Innovation 593, 596 (2018). The program, called PhotoDNA, relies on "hashing" technology to identify known images of CSAM. App'x at 122. When an image is uploaded to Kik, PhotoDNA automatically assigns it "a specific alphanumeric number, known as a hash I.D." or "hash value." App'x at 318. The hash value "serves to identify an individual digital file as a kind of 'digital fingerprint.'" App'x at 70 n.1 (quoting *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011)). PhotoDNA's "database is populated with hash values provided by NCMEC of known images of child pornography." App'x at 70. When an image is assigned a hash value, that value is "matched against a repository provided by NCMEC and if . . . that [hash value] is identified with something in NCMEC's repository, that's how" Kik identifies it as CSAM. App'x at 318; *see also* App'x at 70.

When PhotoDNA "identif[ies] contraband" on Kik, a designated Kik employee personally reviews the file. App'x at 347-48. If the designated employee confirms the file to be suspected child pornography, "he makes a report to NCMEC." App'x at 348. The file is "taken off the public platform

immediately" but at that time, it "is still in the user account." App'x at 349-50. The contraband file is retained by Kik "on the private side of" the system for 90 days for purposes of preservation of evidence. App'x at 350.

The file is also sent to NCMEC, along with "[s]ubscriber data information . . . and activity logs" for the user whose account contained the file. App'x at 319.[3] This reporting is mandatory; the law requires an ESP to report suspected CSAM to NCMEC if the ESP has "actual knowledge" that such material resides on its platform. *See* 18 U.S.C. §2258A(a)(1)(A)(i), (B). Once the PhotoDNA program returns a match and the designated employee reviews the file, Kik has such actual knowledge and must report to NCMEC. Failure to report a file containing CSAM of which the ESP has actual knowledge can be punished by a fine of up to $850,000 for the first failure and $1,000,000 for any subsequent failure. *See id.* §2258A(e). The law does not, however, "require a provider to . . . affirmatively search, screen, or scan" for CSAM. *Id.* §2258A(f)(3).

When NCMEC receives a report through the CyberTipline, it is statutorily obligated to make that report "available to the appropriate law enforcement

[3] Kik is "registered" with NCMEC, meaning that it may file CyberTipline reports through a secure, encrypted channel. App'x at 285.

agency for its review and potential investigation." 34 U.S.C. §11293(b)(1)(K)(i)(II); *see also* App'x at 301. The report generated by NCMEC follows a standardized format; Section A details the information reported by the ESP, and Sections B and C set forth additional information provided by NCMEC. *See, e.g.*, App'x at 90. Section D lists the contact information of the law enforcement agency to whom the report was provided. *See* App'x at 90.

Section B provides information that is "automatically generated by NCMEC Systems," including the file name for any files designated as a "hash match" and a categorization of those files. App'x at 95. "The 'Hash Match' designation indicates that the uploaded file matches the hash value of an uploaded file from a CyberTipline report that was previously viewed and categorized by NCMEC." App'x at 95. Possible categorizations include "Apparent Child Pornography," "Child Unclothed," and "CP (Unconfirmed)." App'x at 108. This section also provides a "Geo-Lookup" for the internet protocol ("IP") address of the user account associated with the suspected CSAM files, and the IP address from which activity involving the files occurred, identifying an internet provider and general geographic location for those IP addresses. *See* App'x at 108. Section C provides "information collected by

NCMEC staff" which may include "data gathered from queries on publicly-available, open-source websites." App'x at 109. Information in Section C is input by "actual human beings . . . as opposed to computer-generated." App'x at 292.

II. The Searches of Guard's Accounts

On September 18, 2020, Kik used the CyberTipline to report seven files containing apparent CSAM to NCMEC. *See* App'x at 89-98 (CyberTipline Report 79722638). According to the Report, on September 16, 2020, an individual using the Kik username "ski18taco" had sent these seven files to other Kik accounts in private chat messages. *See* App'x at 91-94. The Report provided the IP address associated with the account assigned username "ski18taco" and indicated that the IP address was located in Queensbury, New York. *See* App'x at 95. It also designated five of the seven files as "hash matches," three of which were identified as "CP (Unconfirmed)" and two of which were identified as "Apparent Child Pornography." App'x at 95.[4]

Based on the location associated with the IP address, NCMEC forwarded the report to the New York State Police, specifically, the Internet Crimes Against

[4] A federal law enforcement agent later reviewed the files and concluded that they constituted "child pornography" as defined by 18 U.S.C. §2256(8). *See infra* pp. 11-12.

Children ("ICAC") taskforce located in Albany, New York. On October 31, 2020, State Police Investigator Brandon Hudson served an administrative summons on Charter Communications, an internet service provider, seeking subscriber information associated with the IP address identified in the September 2020 Report. Charter reported that the IP address had been assigned to Guard's account from March 17, 2019, through October 28, 2020. *See* App'x at 741-42. Charter also provided a service address in Queensbury, New York. *See* App'x at 741. Another law enforcement agent later obtained lease agreements confirming that Guard had resided at the Queensbury address provided by Charter "from January 15, 2019[,] to November 30, 2020." App'x at 79.

On January 21, 2021, Kik filed a second CyberTipline Report relevant to Guard, attaching 18 files containing apparent CSAM. *See* App'x at 99-111 (CyberTipline Report 84703878). Kik reported that an individual using the Kik username "ski118taco"[5] had shared these files with other Kik accounts, by private or group message, between December 27, 2020, and December 31, 2020. *See* App'x at 101-08. The messages were sent from an IP address located in

[5] The username identified in the January 2021 report – ski**118**taco – is one character different from the username identified in the September 2020 Report – ski**18**taco.

Queensbury, New York, though not the same IP address identified in the September 2020 Report. *See* App'x at 76-77.

NCMEC forwarded the January 2021 Report to the Albany ICAC taskforce. The Report identified six of the files as hash matches, four of which were categorized by NCMEC as "Apparent Child Pornography," one as "CP (Unconfirmed)," and one as "Child Unclothed." App'x at 108.

On February 26, 2021, Investigator Ryan Maestro served an administrative summons on Charter Communications seeking subscriber information for the IP address in the January 2021 Report. *See* App'x at 76-77. Charter responded that the subscriber was Wesley Guard, and the IP address at issue had been assigned to his "account from October 29, 2020[,] until March 2, 2021." App'x at 77. Charter also provided a physical address in Queensbury, New York. *See* App'x at 77. Maestro also ran a criminal history check on Guard; when he discovered a 2011 conviction for Sexual Misconduct, Maestro checked the New York Sex Offender Registry and confirmed that Guard was listed as living at the address provided by Charter. *See* App'x at 78.

Special Agent James Hamilton of the United States Immigration and Customs Enforcement Office of Homeland Security Investigations ("HSI"), who

worked with the Albany ICAC taskforce, "reviewed the files that Kik reported to NCMEC," App'x at 72, and determined that four of the files identified in the September 2020 Report and seven of the files identified in the January 2021 Report "depict[ed] child pornography as defined by 18 U.S.C. §2256," App'x at 72, 75.

On April 27, 2021, a federal judge issued a search warrant for Guard's residence "for evidence of the possession, distribution, and receipt of child pornography." App'x at 80-81. The warrant was executed on April 29, 2021. "Just prior to the execution of the search at Guard's residence," Hamilton, Maestro, and State Police Investigator Thomas Gibney approached Guard at his place of employment and brought him to a State Police facility. App'x at 80.

"At the station, [Hamilton] read [Guard] a *Miranda* warning from an Immigration and Customs Enforcement form, which [Guard] initialed as it was being read to him."[6] App'x at 80-81. Guard "then signed a written waiver of his *Miranda* rights, which also was signed as witnessed by" Hamilton and Maestro. App'x at 81. Guard was then interviewed by the officers. During the interview, Guard stated that he had used Kik in the past, having had two or three accounts

[6] *See Miranda v. Arizona*, 384 U.S. 436 (1966).

over time, but that he had stopped using it "[t]hree, four months ago." App'x at 750. Guard recalled that he had used the usernames "ski18taco" and "ski118taco," and also identified a third username, "the18taco," of which law enforcement was previously unaware. *See* App'x at 766. Guard admitted that he had seen child pornography in the chat rooms, *see* App'x at 754, and that he had been "looking at child pornography" for a while, but "not long," App'x at 758. Guard also agreed that he had "uploaded child pornography into a group using" his Kik accounts, App'x at 756 — specifically, that he had shared child pornography images among various Kik groups, *see* App'x at 759.

On June 14, 2021, Hamilton secured a warrant to obtain "subscriber information, text message content, picture message content, video message content, and any and all images generated in the Kik accounts, including metadata," regarding the three Kik usernames acknowledged by Guard in his interview. App'x at 85. Kik produced records, including hundreds of "pages of user log activity . . . in response to that warrant." App'x at 321.

III. Procedural History

On April 29, 2021 – the date of his interview by law enforcement – Guard was arrested on a criminal complaint charging him with distribution of child

pornography in violation of 18 U.S.C. §2252(a)(2) and (b)(1). *See* App'x at 4. On March 31, 2022, a grand jury returned a six-count indictment charging Guard with three counts of distribution of child pornography in violation of 18 U.S.C. §2252A(a)(2)(A) (Counts 1-3), one count of transportation of child pornography in violation of §2252A(a)(1) (Count 4), one count of receipt of child pornography in violation of §2252A(a)(2)(A) (Count 5), and one count of possession of child pornography in violation of §2252A(a)(5)(B) (Count 6). *See* App'x at 23-27.

On December 2, 2022, Guard filed a motion to suppress. *See* App'x at 28-62. He moved to suppress the electronic communications seized by Kik and transmitted to NCMEC, asserting that because NCMEC is a governmental entity and Kik acted as NCMEC's agent or instrument when it viewed his electronic data, Kik's conduct implicated the Fourth Amendment. Because Kik conducted the search without a warrant, Guard argued, the search was unlawful. Guard also moved to suppress the statements he made in the April 29, 2021, interview with law enforcement, asserting that (1) the officers had failed to properly advise him of his *Miranda* rights, thereby rendering his waiver of those rights void; (2) the officers used unconstitutionally coercive tactics during the interview; and (3) Guard had invoked his right to remain silent, which the officers ignored.

The District Court denied Guard's motion. It agreed with Guard that "NCMEC is likely a government entity or acting as an agent of the government" but refused to extend that status to Kik on the ground that "Kik is a private company with considerably different obligations under the law." Special App'x at 16. The District Court held that the review conducted by Kik therefore did not violate Guard's Fourth Amendment rights. It also held that Guard had validly waived his *Miranda* rights, that the statements he made during the April 29, 2021, interview were not the product of coercion, and that he had not unequivocally invoked his right to counsel in the interview.

The matter proceeded to trial and on February 24, 2023, the jury returned a verdict acquitting Guard on Counts 2 and 3 and convicting him on Counts 4, 5, and 6.[7] Guard filed a motion for acquittal or a new trial, arguing that "the government failed to establish the element of knowledge required for Counts 4, 5, and 6" and "failed to establish [he] had access to the account relating to the possession in Count 6 on or around the date alleged." App'x at 816. The motion was denied. Guard was sentenced principally to 151 months of imprisonment to be followed by 15 years of supervised release.

[7] Count 1 was dismissed on the government's motion prior to trial. *See* Special App'x at 2 n.1.

DISCUSSION

Guard makes four arguments on appeal: (1) the District Court erred by denying his motion to suppress; (2) the trial evidence was insufficient to sustain the convictions; (3) the District Court imposed a substantively unreasonable sentence; and (4) the written judgment does not conform to the District Court's oral pronouncement of the terms of supervised release. We address each in turn.

I. Motion to Suppress

"On appeal from the denial of a motion to suppress, we review a district court's findings of fact for clear error and its legal rulings *de novo*." *Maher*, 120 F.4th at 306. We also review *de novo* "mixed questions of law and fact, including the ultimate determination of whether the admitted or established facts satisfy the relevant statutory or constitutional standard." *United States v. Fiseku*, 915 F.3d 863, 869 (2d Cir. 2018) (citation and quotation marks omitted); *see also United States v. Davis*, 326 F.3d 361, 365 (2d Cir. 2003) (reviewing suppression ruling *de novo* where "parties do not dispute the relevant facts[] but rather whether those facts gave rise to an unlawful search and seizure").

A. Guard's Fourth Amendment Argument

Guard contends that Kik acted as a governmental agent or instrument

when it reviewed his accounts and seized his electronic communications and files "because NCMEC is a government entity and Kik was acting in coordination with NCMEC." Appellant's Br. at 50. Thus, Guard argues, Kik was required to obtain a warrant before searching his accounts and its failure to do so renders the fruits of those searches inadmissible. *See id.* at 58.

"It is axiomatic that the party moving to suppress bears the burden of establishing that his . . . Fourth Amendment rights were violated by the challenged search or seizure. That burden includes satisfying the threshold requirement that the search at issue constituted a governmental action, such that the search implicated the defendant's rights under [the] Fourth Amendment." *United States v. Hines*, 140 F.4th 105, 112 (2d Cir. 2025) (citations and quotation marks omitted). We agree with Guard that NCMEC is a governmental entity for Fourth Amendment purposes. But *Kik*, not NCMEC, searched Guard's electronic data, and Guard has not met his burden of showing that *Kik's* actions implicated the Fourth Amendment. Accordingly, we conclude that the District Court properly denied Guard's motion to suppress.

1. The Fourth Amendment Governs State Action.

The Fourth Amendment guarantees the right to be free from "unreasonable searches and seizures." U.S. Const. amend. IV. It "proscrib[es]

only governmental action," *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), and "does not protect against searches or seizures effected by a private party on her own initiative," *United States v. Cacace*, 796 F.3d 176, 189 (2d Cir. 2015) (per curiam) (citation and quotation marks omitted). However, "[t]he Constitution constrains governmental action by whatever instruments or in whatever modes that action may be taken." *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 392 (1995) (citations and quotation marks omitted). "[A] state may not induce, encourage[,] or promote private persons to accomplish what it is constitutionally forbidden to accomplish." *Norwood v. Harrison*, 413 U.S. 455, 465 (1973) (citation and quotation marks omitted). Accordingly, "[a] search conducted by private individuals at the instigation of a government officer or authority may sometimes be attributable to the government for purposes of the Fourth Amendment, but private actions are generally attributable to the government only where there is a sufficiently close nexus between the State and the challenged action of the entity so that the action of the latter may be fairly treated as that of the State itself." *United States v. DiTomasso*, 932 F.3d 58, 67-68 (2d Cir. 2019) (citations and quotation marks omitted). "Thus, a private search or seizure may implicate the Fourth Amendment where the private party acts 'as an agent

of the Government or with the participation or knowledge of any governmental official.'" *United States v. Rosenow*, 50 F.4th 715, 728-29 (9th Cir. 2022) (quoting *Jacobsen*, 466 U.S. at 113).

The Supreme Court has addressed "the question [of] whether particular conduct is 'private,' on the one hand, or 'state action,' on the other," *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 349-50 (1974), and "has articulated a number of different factors or tests in different contexts," *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 939 (1982). "Sometimes, the Court uses a 'function' test that asks whether a private party performs a public function. Other times, the Court uses a 'compulsion' test that asks whether the government compelled a private party's action. Still other times, the Court uses a 'nexus' test that asks whether a private party cooperated with the government." *United States v. Miller*, 982 F.3d 412, 422 (6th Cir. 2020) (citations omitted).

In other words, there are several ways in which a private party's conduct may be "fairly attributable" to the government for Fourth Amendment purposes. *Lugar*, 457 U.S. at 937. The determination of whether a given search triggers Fourth Amendment protection is "fact-bound." *Id.* at 939. "What is fairly attributable" to the government under the circumstances "is a matter of

normative judgment, and the criteria lack rigid simplicity." *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295 (2001).

As the party seeking suppression, Guard "bears the burden of demonstrating that the private party conducting the search was acting as an instrument or agent of the government," *Hines*, 140 F.4th at 113, "such that the search implicated [his] rights under [the] Fourth Amendment," *id.* at 112. This is a threshold requirement. If Guard can establish that the Fourth Amendment applies to Kik's search but no warrant was obtained, the burden would shift to the government to demonstrate that "the search was valid because it fell within one of the exceptions to the warrant requirement." *United States v. Perea*, 986 F.2d 633, 639 (2d Cir. 1993).

2. NCMEC Is a Governmental Entity.

Guard contends that the evidence discovered by Kik should be suppressed because Kik acted as a governmental agent or instrument by "acting in coordination with NCMEC." Appellant's Br. at 53. Before we consider Kik's conduct, we first consider whether NCMEC itself is a governmental entity. We conclude that the federal regulatory scheme that governs NCMEC's operations and structure renders it a governmental entity for Fourth Amendment purposes.

NCMEC is a private nonprofit corporation established "to help find missing children, reduce child sexual exploitation, and prevent child victimization." App'x at 67. But its private corporate status does not end the inquiry. The Supreme Court has "treated a nominally private entity as a state actor when it is controlled by an agency of the State, when it has been delegated a public function by the State, when it is entwined with governmental policies, or when government is entwined in its management or control." *Brentwood*, 531 U.S. at 296 (citations and quotation marks omitted). The Court's "cases are unequivocal in showing that the character of a legal entity is determined neither by its expressly private characterization in statutory law, nor by the failure of the law to acknowledge the entity's inseparability from recognized government officials or agencies." *Id.* Put simply, the question is one of function over form; it "turn[s] on what the entity does, not how it is organized." *United States v. Ackerman*, 831 F.3d 1292, 1295 (10th Cir. 2016).

"[T]he calling card of a governmental entity is whether it is invested with any portion of political power, partaking in any degree in the administration of civil government, and performing duties which flow from the sovereign authority." *Id.* (citation and quotation marks omitted). The statutory scheme

that governs NCMEC's activities imbues it with "political power" and "sovereign authority" such that, when NCMEC performs its statutory functions, it does so as a governmental entity. *Id.*

Congress has empowered NCMEC to exercise significant law enforcement responsibility, a paradigmatic feature of state power. *See Foley v. Connelie*, 435 U.S. 291, 297 (1978) (describing the "police function" as "one of the basic functions of government"). Its primary authorizing statutes — 18 U.S.C. §2258A and 34 U.S.C. §11293 — require it to collaborate with law enforcement "in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person." *Ackerman*, 831 F.3d at 1296. By this allocation of authority, Congress has positioned NCMEC as a linchpin in the law enforcement system for the investigation of crimes against children. NCMEC not only operates a national 24-hour call center, the AMBER Alert Secondary Distribution Program, and the CyberTipline, but also is obliged to ensure that all reports of child exploitation are provided to the appropriate law enforcement agency. *See* 34 U.S.C. §11293(b)(1)(A), (K). And ESPs "must report any known child pornography violations to NCMEC. Not to any other governmental agency, but . . . to NCMEC and NCMEC alone." *Ackerman*, 831

F.3d at 1296. Congress also has granted NCMEC statutory immunity, authorizing it to knowingly receive and view CSAM and to distribute otherwise illegal materials to law enforcement agencies. *See* 18 U.S.C. §2258A(g)(3). These are "[a]ctions that would normally subject private persons to criminal prosecution . . . [b]ut . . . that Congress allows NCMEC to take precisely because of the unique value it provides in the prosecution of child exploitation crimes." *Ackerman*, 831 F.3d at 1297 (citations omitted).

The history of NCMEC's creation confirms its status as a governmental entity for purposes of the Fourth Amendment analysis. In 1984, Congress enacted the Missing Children's Assistance Act ("MCAA"), which authorized grants and contracts "with public agencies or nonprofit private agencies" to establish and "operate a national resource center and clearinghouse designed"

> (A) to provide technical assistance to local and State governments, public and private nonprofit agencies, and individuals in locating and recovering missing children;
>
> (B) to coordinate public and private programs which locate, recover, or reunite missing children with their legal custodians;
>
> (C) to disseminate nationally information about innovative and model missing childrens' programs, services, and legislation; and
>
> (D) to provide technical assistance to law enforcement agencies, State and local governments, elements of the criminal justice system, public and private nonprofit agencies, and individuals in the prevention,

> investigation, prosecution, and treatment of the missing and exploited child case.

Pub. L. 98-473, §404, 98 Stat. 1837 (1984).

In 1999, Congress amended the MCAA by enactment of the Missing, Exploited, and Runaway Children Protection Act. *See* Pub. L. 106-71, 113 Stat. 1032 (1989). The 1999 Act supplemented the findings section of the MCAA to explicitly state that for "14 years, the National Center for Missing and Exploited Children has served as the national resource center and clearinghouse congressionally mandated under the provisions of the Missing Children's Assistance Act of 1984." *Id.* §2. The 1999 Act also struck the reference in the MCAA to grants and contracts generally, replacing it with a directive to fund NCMEC to accomplish the designated tasks. *See id.* Today, NCMEC remains the sole entity empowered to "operate the official national resource center and information clearinghouse for missing and exploited children." 34 U.S.C. §11293(b)(1)(B). Accordingly, we conclude that NCMEC constitutes a governmental entity for Fourth Amendment purposes.

3. Guard Has Not Established That Kik Acted as a Governmental Agent or Instrument When It Searched His Accounts.

We now turn to Kik. Guard argues "[t]here was a sufficiently close nexus

to attribute Kik's searches to the government because . . . Kik was acting in coordination with NCMEC." Appellant's Br. at 50. We construe this as asserting that Kik's search was "attributable to the government" because there was "a sufficiently close nexus between the State and the challenged action of the entity so that the action of the latter [(Kik)] may be fairly treated as that of the State itself." *DiTomasso*, 932 F.3d at 67-68 (citation and quotation marks omitted).[8]

"The close nexus test is not satisfied when the state merely approves of or acquiesces in the initiatives of the private entity. Instead, a close nexus is generally found when the state exercises coercive power, is entwined in the management or control of the private actor, or provides the private actor with significant encouragement, either overt or covert." *Hines*, 140 F.4th at 112 (citation and quotation marks omitted). "The purpose of the close-nexus requirement is to assure that constitutional standards are invoked only when it

[8] As noted above, the "close nexus" test is not the only one under which we may assess whether a search by a private actor triggers Fourth Amendment protections. *See, e.g.*, *Miller*, 982 F.3d at 422 (describing the public function, compulsion, and nexus tests, all of which have been employed by the Supreme Court in this context). It is, however, the only test that Guard argues on appeal should be applied. While Guard's brief mentions the compulsion test in passing, it makes no argument that Kik was coerced or compelled by NCMEC to conduct the searches. *See* Appellant's Br. at 53-54. But in any event, Guard did not produce evidence that Kik was coerced or compelled.

can be said that the government is *responsible* for the specific conduct of which the accused complains." *DiTomasso*, 932 F.3d at 68 (citation and quotation marks omitted). Guard contends that "Kik's nexus with the government" is established by the fact that "Kik searches its database only for the hash values that are provided to it by NCMEC and entered into the PhotoDNA program that is used to scour through databases." Appellant's Br. at 56 (quotation marks omitted). "Kik's use of hash values supplied solely by NCMEC," he argues, "transformed it into a government agent." *Id.*

As noted, it was Guard's "burden to establish that the search violated his Fourth Amendment rights." *United States v. Lewis*, 62 F.4th 733, 741 (2d Cir. 2023). The evidence revealed that PhotoDNA, the software used by Kik to detect CSAM, makes use of data provided by NCMEC; accordingly, Guard established at trial that Kik was running searches against a database provided by a governmental entity. But Guard cannot carry his burden based on this fact alone. The evidence presented in this case does not establish any further involvement by NCMEC in Kik's decision to deploy the software or in Kik's use of the software. The evidence in this case does not establish whether and how NCMEC communicates with Kik about its use of PhotoDNA or provides "significant

encouragement" to use it. *Hines*, 140 F.4th at 112. Nor does the evidence admitted before the District Court show that NCMEC owns the PhotoDNA software or controls Kik's access to the software. The record in this case reveals only that NCMEC makes a database available, PhotoDNA uses that database to detect suspected CSAM, and Kik applies PhotoDNA to search files on its platform for matches to the files included in NCMEC's database. More is required to establish a sufficiently "close nexus" between NCMEC and Kik's search to trigger the protection of the Fourth Amendment.

In sum, we find that Guard failed to carry his burden of showing that Kik acted as a governmental agent when it searched his accounts for child pornography and provided the materials it found in his accounts to NCMEC.[9] That finding forecloses Guard's Fourth Amendment challenge. We therefore find no error in the denial of his motion to suppress this evidence.

B. Guard's Fifth Amendment Argument

Next, Guard argues that the District Court should have suppressed the statements he made in his April 29, 2021, interview with law enforcement

[9] Our holding is limited to the facts of this case and to the question of whether Guard presented sufficient evidence to establish that Kik's search triggered Fourth Amendment protection.

because "his *Miranda* rights were not reasonably conveyed or voluntarily and knowingly waived." Appellant's Br. at 64. "We review a district court's determination regarding the constitutionality of a *Miranda* waiver *de novo* . . . [and the] district court's underlying factual findings for clear error." *United States v. Capers*, 627 F.3d 470, 474 (2d Cir. 2010) (citation and quotation marks omitted). We find that the District Court did not commit clear error in finding, as a matter of fact, that HSI Special Agent Hamilton informed Guard of his *Miranda* rights. We also conclude that Guard knowingly and voluntarily waived them.

Before beginning a custodial interrogation, law enforcement must inform the suspect that he has the right to remain silent, that anything he says can be used against him in a court of law, that he has the right to an attorney, and that if he cannot afford an attorney, one will be appointed for him. *See Miranda v. Arizona*, 384 U.S. 436, 467-73, 479 (1966). However, an individual "may waive effectuation of these rights, provided the waiver is made voluntarily, knowingly[,] and intelligently." *United States v. Medunjanin*, 752 F.3d 576, 586 (2d Cir. 2014) (citation and quotation marks omitted).

Before he was questioned, Guard signed a form waiving his *Miranda* rights. Guard contends that this waiver was ineffective because Hamilton did

not accurately explain the right to counsel.[10] *See* Appellant's Br. at 63. Guard asserts that the following exchange reveals that he did not understand his rights:

> **Hamilton:** And here's the most important one: If you decide to answer questions now, you still have the right to stop questions at any time or to stop the questions for the purpose of consulting an attorney. And then this is the waiver so that I can talk to you and kind of explain what's going on. It says that you've read or someone's read to you the statement of rights and you understand what your rights are, and at this time you are willing to answer questions without a lawyer present.
>
> **Guard:** Okay. (Witness initials)
>
> **Hamilton:** I want to just note the time that –
>
> **Guard:** Hold on one second. If I ask for a lawyer during questioning, can I get one or . . .
>
> **Hamilton:** Um, we can work on that, yes.
>
> **Guard:** Okay.
>
> **Hamilton:** And, basically, what that last, the waiver and what that last statement says, that if you don't want to answer questions now, we can stop and, you know, bridge that gap if we need to.
>
> **Guard:** Okay.

---

[10] In the District Court, Guard advanced two additional bases for suppression of the statements: first, that Hamilton employed unduly coercive interview tactics, and second, that Hamilton ignored his unequivocal invocation of the right to silence and continued the interview. *See* App'x at 50-57. Guard does not pursue these arguments on appeal, and we therefore do not address them. *See Hussein v. Maait*, 129 F.4th 99, 123 (2d Cir. 2025) ("Arguments not made in an appellant's opening brief are waived even if the appellant pursued those arguments in the district court." (citation and quotation marks omitted)).

App'x at 748. We do not agree that this exchange undermines the validity of the waiver. Guard was able to ask an informed question; he was advised that he could stop the interview if he wished, and that a lawyer could be obtained for him. He acknowledged Hamilton's response and proceeded to complete the waiver form and answer Hamilton's questions. We conclude that Guard knowingly and voluntarily waived his *Miranda* rights. Accordingly, the District Court did not err in declining to suppress the statements following this waiver.

II. Sufficiency of the Evidence

Guard raises two challenges to the sufficiency of the evidence against him at trial. He argues, first, that "the evidence was insufficient to show that he knew each file contained child pornography as required by the fourth element of each count" of the indictment, and, second, "that the government failed to prove that any access he had to child pornography was substantially close in time to April 29, 2021, as charged in Count Six." Appellant's Br. at 36.

Although we review challenges to the sufficiency of the evidence *de novo*, the defendant "bears a heavy burden." *United States v. Aquart*, 912 F.3d 1, 17 (2d Cir. 2018); *see also United States v. Jimenez*, 96 F.4th 317, 324 (2d Cir. 2024). "[W]e will sustain the jury's verdict if *any* rational trier of fact could have found the

essential elements of the crime beyond a reasonable doubt." *United States v. Gu*, 8 F.4th 82, 86 (2d Cir. 2021) (citation and quotation marks omitted); *see also United States v. Ramos*, 685 F.3d 120, 130 (2d Cir. 2012).

A. Knowledge

Each count of conviction requires proof that the defendant knew that the visual depiction in the file at issue was of (1) an actual minor (2) engaged in sexually explicit conduct. *See United States v. Colavito*, 19 F.3d 69, 71 (2d Cir. 1994). Knowledge is "provable (as knowledge must almost always be proved) by circumstantial evidence." *United States v. Santos*, 553 U.S. 507, 521 (2008). While Guard concedes the visual depictions are child pornography, he argues that "[t]he government failed to prove beyond a reasonable doubt that [he] knew the visual depictions connected to his Kik accounts contained child pornography" at the time he possessed them. Appellant's Br. at 38. Specifically, he contends that the government presented no evidence showing that he knew the file names, that the context of the transmission of the files indicated knowledge that they contained child pornography, or that he ever actually opened or viewed the files. He emphasizes that on Kik, "[v]ideo files appear as thumbnails, depicting a still from someplace in the video," and "there was no basis to conclude that the

thumbnails themselves depicted child pornography." *Id.* at 38-39.

We conclude that a rational factfinder could find, based on the evidence presented at trial, that Guard knew the materials constituted child pornography. Indeed, the trial evidence revealed that Guard *admitted* to SA Hamilton that he had been looking at child pornography on Kik for a period of time. *See, e.g.*, App'x at 758 ("Q. And how long have you been looking at child pornography? A. Not long.").

Therefore, we conclude that the trial evidence sufficed to establish Guard's knowledge. Guard presented an alternative perspective on the evidence presented at trial. But a reasonable jury could – and did – reject his interpretation.

B. Possession

The indictment alleged in Count 6 that Guard had possessed child pornography "[o]n or about April 29, 2021." App'x at 24. Guard argues that there was no evidence produced at trial proving "that [he] possessed child pornography or had access to any Kik account containing child pornography past December 31, 2020." Appellant's Br. at 42. The jury appears to have struggled with this question, sending in a note asking: "When was each Kik

account banned?" App'x at 707. In response, the District Court provided a readback of testimony it determined was relevant to that question. *See* App'x at 707. The jury also requested an opportunity to view the entire video of Guard's interview by SA Hamilton. *See* App'x at 690.

The government contends that the evidence is sufficient to support a verdict of possession on or about April 29, 2021 – the date charged in the indictment – because Guard remained able to "exercise dominion and control over" the images in April 2021, even if he did not actually access them. Appellee's Br. at 31 (quoting *Ramos*, 685 F.3d at 132). Guard asserts that there was "no evidence indicating" whether that "account was still active or whether it was banned," and no evidence of whether "any file containing child pornography remained in" that account after "December 31, 2020, and, if so, whether it was accessible to Guard." Appellant's Br. at 43.

The evidence at trial was as follows. In late December 2020, Guard used his "ski118taco" account to send at least five files containing CSAM to his "the18taco" account. *See* App'x at 730. A representative of Kik testified that the "the18taco" account would have been banned if Kik were aware that it had been used to share child pornography, but that if it only *received* such materials it

would not be banned.[11] *See* App'x at 353, 364. At trial, the government introduced a transcript of selected portions of the April 29, 2021, interview by SA Hamilton with Guard. *See United States v. Guard*, 1:22CR00105(MAD) (N.D.N.Y. Feb. 24, 2023), Doc. #106 at 2 (list of government exhibits indicating that Exhibit 8MT was admitted into evidence). That transcript reflects that Hamilton asked Guard whether he had ever used his "the18taco" account to share child pornography, and Guard said: "No. I just trolled people with it." App'x at 766 (Exhibit 8MT). Hamilton then confirmed that "[i]t was just the other two accounts" that Guard used for that purpose. App'x at 766 (Exhibit 8MT).

Thus, the jury had before it evidence that Guard had access to the "the18taco" account in late 2020; that it was not used to share child pornography; and that an account that had not been used to share child pornography would not have been banned. This is not strong evidence that Guard retained access to the account in April 2021. But "[w]e will not vacate a conviction on sufficiency of

[11] Of course, an account would not be banned if it never came to Kik's attention as being involved with suspected CSAM. The record in this case does not indicate that Kik ever submitted a report to NCMEC regarding the "the18taco" account, and in fact suggests the absence of any such report, given that law enforcement were unaware of the account. It is reasonable to infer based on the record that Kik never identified "the18taco" as an account trafficking in contraband files.

the evidence grounds if, drawing all inferences in favor of the prosecution and viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Santos*, 449 F.3d 93, 102 (2d Cir. 2006) (citation and quotation marks omitted) (emphasis omitted). The jury could infer, from the evidence presented, that the account remained accessible to Guard on April 29, 2021.

IV. Substantive Reasonableness of Sentence

On July 28, 2023, the District Court sentenced Guard principally to 151 months of incarceration to be followed by a 15-year term of supervised release. Guard contends that the sentence was substantively unreasonable because the District Court failed to "seriously consider[] the guidelines' flaws" and "gave no indication that it considered any of Guard's mitigating factors." Appellant's Br. at 67, 68.

"We review the district court's sentencing decision for 'reasonableness,' which is essentially review for abuse of discretion." *United States v. Skys*, 637 F.3d 146, 152 (2d Cir. 2011). "[O]nly those sentences that are so shockingly high, shockingly low, or otherwise unsupportable as a matter of law that allowing

them to stand would damage the administration of justice" will be set aside as substantively unreasonable. *United States v. Muzio*, 966 F.3d 61, 64 (2d Cir. 2020) (citation and quotation marks omitted).

At sentencing, Guard urged the District Court to consider certain mitigating factors, such as the short duration of his offense conduct, the small number of files Guard accessed, the fact that Guard did not maintain a collection of child pornography or store such images on his digital devices, and Guard's status as a married father of two at the time of the offense.[12] *See* Appellant's Br. at 68; *see also* App'x at 916-17. Even accepting the accuracy and relevance of these facts, however, the 151-month prison sentence is not substantively unreasonable. Counts 4 and 5 each carried a statutory mandatory *minimum* of 60 months of imprisonment; all three counts of conviction carried statutory *maximums* of 20

[12] In imposing sentence, the District Court did not expressly comment on these arguments. But that is not sufficient to establish error; we do not "insist that the district court address every argument the defendant has made or discuss every §3553(a) factor individually" on the record, *United States v. Villafuerte*, 502 F.3d 204, 210 (2d Cir. 2007), and Guard does not cite any other evidence suggesting the District Court failed to consider mitigating factors. The District Court heard argument from Guard's attorney, and it made clear that it had reviewed the PSR and the parties' submissions. Moreover, the District Court imposed a term of imprisonment well below the statutory maximum and 17 months below the bottom of the range recommended by the Guidelines, suggesting that mitigating factors played at least some role in its determination.

years in prison. The statutorily authorized range of sentences was therefore five to sixty years of imprisonment. The statutes of conviction also authorized a supervised release term of at least five years and up to life. The Guidelines recommended a sentence of 168 to 210 months of imprisonment, and a lifetime term of supervised release.

The record shows that the District Court adequately considered and applied the §3553(a) factors. It considered the nature of the offense and impact on victims. *See* App'x at 921. The court read into the record descriptions of the videos found in Guard's possession, as well as comments made by other Kik users in response to the images that Guard offered to share. The District Court also discussed Guard's prior conviction for sexual misconduct involving a minor, his violations of pretrial release, and his mental health.

In light of the totality of the circumstances, including the facts recited by the Court *and* those emphasized by Guard, and the range of available sentences, we conclude that the sentence imposed is not substantively unreasonable. *See Gall v. United States*, 552 U.S. 38, 51 (2007). Although Guard points to mitigating factors that he feels were undervalued, we will not "second guess the weight (or lack thereof) that the judge accorded to a given factor or to a specific argument

made pursuant to that factor." *United States v. Degroate*, 940 F.3d 167, 178 (2d Cir. 2019) (citation and quotation marks omitted).

With respect to the District Court's application of U.S.S.G. §2G2.2, it is true that, in the context of child pornography, the Guidelines must be "applied with great care" to prevent the imposition of unreasonable sentences inconsistent with the dictates of 18 U.S.C. §3553(a). *United States v. Jenkins*, 854 F.3d 181, 188 (2d Cir. 2017). The District Court expressly considered this issue at sentencing. Indeed, the District Court discussed in detail the nature of the concerns with Section 2G2.2, and stated that it was considering each of the offense-level increases recommended by that section "directly related to the specific crime . . . that is charged in the case." App'x at 903. The District Court also declined to impose an increase of two offense levels for distribution sought by the government. *See* App'x at 917. And of course, the District Court imposed a sentence that was below the bottom of the Guidelines' recommended range. On this record, we conclude that Guard's sentence does not fall outside the range of permissible decisions.

V. Conditions of Supervised Release

Guard argues that the written judgment does not conform with the District

Court's oral pronouncement of Special Conditions 2, 3, 4, and 7. We agree as to three of these conditions and remand with instructions for the District Court to amend the written judgment to conform with the oral pronouncement of Special Conditions 2, 4, and 7.

"We review de novo the asserted discrepancy between the spoken and written terms of [a] sentence." *United States v. Washington*, 904 F.3d 204, 207 (2d Cir. 2018). "[W]here an unambiguous oral sentence conflicts with the written judgment, . . . the oral pronouncement of sentence must control. When such a conflict exists, the proper remedy is to remand for amendment of the written judgment." *United States v. Peguro*, 34 F.4th 143, 165 (2d Cir. 2022) (citations and quotation marks omitted).

As written, Special Condition 2 provides in relevant part that Guard "shall not have direct contact with any child you know or reasonably should know to be under the age of 18 without the permission of the probation officer." Special App'x at 73. Special Condition 4 provides that Guard "shall not go to, or remain at, a place for the primary purpose of observing or contacting children under the age of 18." Special App'x at 73. At sentencing, however, the District Court stated that the Special Conditions imposed would not prohibit Guard from having

contact with his own minor children. Thus, remand is warranted to amend the written judgment with respect to Special Conditions 2 and 4 because the written judgment does not make clear that these conditions do not prohibit Guard from contact with his own minor children.

As written, Special Condition 3 provides that Guard "shall not go to, or remain at, any place where you know children under the age of 18 are likely to congregate, including parks, schools, playgrounds, and childcare facilities without the permission of the probation officer." Special App'x at 73. This does not conflict with the oral pronouncement of Special Condition 3. Nothing in the record indicates that the District Court intended to allow Guard's contact with his children to occur at a place where other children congregate. Thus, the scope of the remand does not include Special Condition 3 because the prohibition on Guard going places where children congregate is not inconsistent with allowing Guard to see his own children.

Finally, Special Condition 7 provides in relevant part that Guard "may be limited to possessing one personal internet capable device." Special App'x at 73. The District Court clarified at sentencing that the one-device limitation in Special Condition 7 would be based "[u]pon recommendation of the probation

department and upon order of the Court." App'x at 934. Thus, remand is again warranted to conform Special Condition 7 with the written judgment to clarify that the District Court, not Probation, will determine whether to limit Guard to a single internet-capable device.

CONCLUSION

For the foregoing reasons, we **AFFIRM IN PART** and **VACATE IN PART** the judgment of the District Court, and **REMAND** with instructions for the District Court to amend the written judgment to conform with the oral pronouncement of Special Conditions 2, 4, and 7, specifically to clarify that Guard is not prohibited from contact with his own minor children and that the District Court, not Probation, will determine whether to limit Guard to a single internet-capable device.