This AI Tool Helped Convict People of Murder. Then Someone Took a Closer Look

Todd Feathers ⋮ 24-30 minutes ⋮ 10/15/2024

Just after 9 pm on an August night in 2020, Kimberly Thompson and Brian James pulled the car into a driveway in Akron, Ohio, and stepped out into a barrage of gunfire. They were shot in the legs, rushed to a hospital, and survived. But Thompson's 20-month-old grandson, Tyree Halsell, who was still sitting in the car, was shot in the head and mortally wounded.

In the aftermath, Akron police collected video footage from the neighborhood and asked for the public's help with identifying two men who'd been seen approaching the victims, firing, then fleeing in a truck. Within months, detectives narrowed in on a suspect, Phillip Mendoza, and obtained a search warrant for his cell phone location data from Sprint, according to court records. They also served a geofence warrant on Google, seeking information on devices whose GPS, Wi-Fi, or Bluetooth records placed them near the scene of the shooting. Neither warrant turned up any evidence locating Mendoza or his devices on the 1200 block of Fifth Avenue, where the shooting occurred, that night.

The investigation stalled until August 2022, when Akron police received a three-page report containing the evidence they'd been seeking. It came from a little-known Canadian company called Global Intelligence, which for the past several years has been selling an extraordinary service to police departments across the United States.

Global Intelligence claims that, using only open source data—public information that doesn't require a warrant—and a suite of more than 700 algorithms, its Cybercheck system allegedly can geolocate an individual in real time or at a specific time in the past by detecting the wireless networks and access points the person's "cyber profile" has interacted with. The company's founder, Adam Mosher, has testified under oath that the process is entirely automated, requiring no human intervention from the time an investigator enters basic details about a case into the Cybercheck portal until the time the system produces a report identifying a suspect and their location.

If the technology works as advertised, then Global Intelligence is selling police departments previously unknown surveillance capabilities for as little as $309 a case that rival the open source tools used by national spy agencies. But a WIRED review of investigations involving Cybercheck from California to New York, based on hundreds of pages of court filings, testimony, interviews, and police records, suggests Cybercheck is a much less effective tool—one that has provided evidence in high-profile cases that was either demonstrably incorrect or couldn't be verified by any other means.

Open source intelligence experts allege to WIRED that much of the information Cybercheck provides in its reports to law enforcement would be impossible to obtain using only open source data. Indeed, over the past several months, Global Intelligence's work in Ohio has faded away, with prosecutors ultimately deciding not to use Cybercheck reports as evidence in several murder cases, including Mendoza's.

“Either they’re somehow doing the *Minority Report* now, or somehow it’s just BS,” says Stephen Coulthart, director of the Open Source Intelligence Laboratory at the State University of New York at Albany, who reviewed Cybercheck reports and transcripts of Mosher’s testimony at WIRED’s request.

Cases Pending

During a November 2022 trial, Mosher testified that 345 different law enforcement agencies had used Cybercheck to conduct approximately 24,000 searches since 2017. WIRED identified more than a dozen cases involving Cybercheck, including 13 in which prosecutors intended to use Cybercheck reports as evidence at trial. Two of the cases in which courts allowed Cybercheck reports to be admitted as trial evidence resulted in murder convictions.

The agencies we found using Cybercheck ranged from small suburban police departments to county sheriffs and state police. The alleged crimes ranged from those related to child sexual abuse material to drive-by shootings, as well as cold cases that have haunted communities for decades. Last year, for example, the New York State Police arrested a man for murder after receiving evidence from Cybercheck that allegedly placed his cell phone at key locations on the night of the homicide, roughly 20 years ago, according to the indictment. The case is scheduled to go to trial in 2025.

While Mosher has testified on numerous occasions about Cybercheck, his explanations of what data sources the algorithms draw on and how they reach their conclusions do not fully explain Cybercheck’s ability to produce its reports. Global Intelligence did not answer WIRED’s questions about who designed Cybercheck’s algorithms or what data the company used to train them. When asked how the tool could determine that a person’s cyber profile had pinged a particular wireless network—oftentimes years after the incident occurred—an unnamed Global Intelligence employee wrote in an email: “There is no specific single source of information with regard to wireless network interactions.”

Accuracy Ratings

In 2022, more than two years after Halsell was shot and killed in Akron, Cybercheck produced a report for police that claimed Mendoza’s cyber profile had pinged two wireless internet devices located near 1228 Fifth Avenue after 9 pm. A cyber profile, from what Mosher has testified, is the amalgamation of names, aliases, emails, phone numbers, IP addresses, Google IDs, and other online identifiers that combine to create a person’s unique digital fingerprint.

Summit County prosecutors charged Mendoza with murder. But when Mendoza’s defense attorney, Donald Malarcik, dug into the Cybercheck report, he found a problem. The police department employee who entered the information into Cybercheck’s system had allegedly made a mistake: They had asked the system whether it could locate Mendoza at the scene on August 20, 2020. The shooting occurred on August 2. Cybercheck had nonetheless claimed to locate Mendoza at 1228 Fifth Avenue with 93.13 percent accuracy, even though it was on the wrong day. Stranger still to Malarcik, at some point after delivering the first report, Cybercheck produced another report. It was identical in all respects to the first report—from the MAC addresses, which are unique IDs assigned to networked devices, to the time of day when Mendoza’s cyber profile allegedly pinged them, and the accuracy rating—except it had

the correct date of the shooting.

The warrants served to Sprint and Google hadn't produced any evidence that Mendoza's devices or accounts were at the scene. But according to Cybercheck's entirely automated algorithms, Mendoza's cyber profile had not only been at 1228 Fifth Avenue at the time of the shooting, it had also been at the exact same location, at the exact same time of day, for the same amount of time, pinging the same wireless networks, 18 days later.

The unnamed Cybercheck employee who responded to WIRED's questions says the company stands by the accuracy of both reports in the Mendoza case. "It is not uncommon to have the same cyber profile with the same device at a location on a different date," they wrote.

Malarcik filed a motion where he asked the prosecutor to provide Cybercheck's software in another case for which a report had been generated. He also subpoenaed Mosher, and hired a digital forensics expert in an attempt to review the code and the two Cybercheck reports about Mendoza. He tells WIRED that all that experts in a separate case allegedly saw were a couple hundred lines of code that created a program for searching public websites for information about a subject—nothing like the 1 million lines of code and more than 700 algorithms Mosher has testified about in pre-trial hearings.

"It was the equivalent of what you would do on a Google search," Malarcik alleges. "What we didn't see is the secret sauce, which [Mosher] claims is the machine learning that takes these data points and turns it into intelligence that takes a cyber profile and says it was at this location. That's what he's never disclosed to us."

Mosher and Global Intelligence did not respond to WIRED's questions about Malarcik's claims.

Malarcik requested the court hold what is known as a Daubert hearing to determine whether Mosher's testimony about Cybercheck's findings was credible enough to be admitted as evidence in Mendoza's trial. Two days before the hearing date, Summit County prosecutors decided to not use Cybercheck as evidence. Since then, the prosecutor's office has withdrawn Cybercheck reports in three other cases, involving four men accused of murder, in which they potentially could have been presented as evidence, according to Malarcik and court records. In early August, Mendoza pleaded guilty and was sentenced to serve at least 15 years of a 15-to-20.5-year sentence.

"In the cases we had with Cybercheck that went to trial, there were those aspects that Cybercheck found that the boots-on-the-ground detectives also found," Brad Gessner, the Summit County prosecutor's chief counsel, tells WIRED. "Those things matched."

In total, the office has used, or intended to use, Cybercheck reports in 10 cases brought to them by the Akron Police Department, Gessner said. The Akron Beacon Journal and NBC News were the first to report about the county's use of the tool.

The Summit County Sheriff's Office confirmed to the Akron Beacon Journal this month that it is investigating whether Mosher lied under oath but provided no other details.

In other cases—murder trials for Salah Mahdi and Adarus Black—defense attorneys didn't challenge the use of Cybercheck and the trials resulted in convictions. Both convictions were

upheld by an appeals court.

Since then, judges overseeing the murder trials of Javion Rankin, Deair Wray, Demonte Carr, and Demetrius Carr have ruled that Cybercheck cannot be admitted as evidence unless Global Intelligence grants the defendants access to its source code. However, the Summit County Prosecutor's Office appealed several of those rulings, and in September an Ohio appeals court ruled that the trial court erred in excluding the Cybercheck reports as evidence for reasons unrelated to the technology's effectiveness.

In other jurisdictions, WIRED found, prosecutors have also decided not to use Cybercheck reports, or have dropped charges against defendants after defense attorneys scrutinized the findings and Mosher's testimony.

In 2021, Midland County, Texas sheriff's deputies were investigating the murder of a woman whose burned body had been found in a roadside field. Deputies had arrested the woman's ex-boyfriend, Sergio Cerna, on unrelated charges. When they searched his phone, according to an affidavit, they found text messages in which he threatened the victim, including texts that read, "Your car is going to be burned down then you will be next." But they couldn't find evidence that placed Cerna near the scene of the crime.

The sheriff's office asked Cybercheck for help and received a report claiming that the algorithms had determined, with 97.25 percent accuracy, that Cerna's cyber profile had pinged a wireless LaserJet printer near the crime scene the day the victim's body was found. Prosecutors wanted to use the report as evidence at Cerna's trial, but his defense requested a Daubert hearing. Halfway through the hearing and before the defense could cross-examine Mosher, assistant district attorney Lisa Borden decided not to use Mosher's testimony or the Cybercheck report at trial.

"We would have needed to be able to authenticate that data," she tells WIRED, but by the time of the Daubert hearing, the printer that Cybercheck had identified in its report couldn't be located. That was the first, and only, Daubert hearing that Cybercheck has been subjected to in the country, according to court records and Global Intelligence.

A Midland County jury convicted Cerna in March and sentenced him to life in prison. Cerna's attorney said he would appeal the conviction.

In Colorado, questions about Mosher and Cybercheck preceded prosecutors' dropping the charges and sealing the file against a defendant in what law enforcement said was a child sexual abuse material (CSAM) case. After learning that the local district attorney's office planned to enter Cybercheck evidence at trial and call Mosher as an expert witness, defense attorney Eric Zale hired private investigators to look into Mosher's background.

Mosher told the Boulder County court that he'd previously testified as an expert witness in two CSAM cases in Canada, according to Zale and an appeal brief filed by Malarcik for another client in which a Cybercheck report had been shared in discovery. But after being contacted by Zale's investigator, the Canadian prosecutors in one of those cases contacted the prosecutor in Boulder County to say that Mosher had never been called to testify in any capacity. The defendant, who was related to Mosher, had pleaded guilty on the first day of the trial. A prosecutor familiar with the other Canadian case wrote to the court that no charges had ever been brought against the person whose trial Mosher had told a judge he testified at.

Zale alleges Mosher is “preying on this kind of holy grail of technology to sucker local law enforcement and judges and prosecutors, and frankly some defense counsel” into relying on Cybercheck’s technology.

Mosher did not respond to WIRED’s request to comment on Zale’s claims. Global Intelligence did not dispute that Mosher claimed to have testified as an expert in the two Canadian cases.

“Mr. Mosher felt at the time that he needed to relay all court participation activities including provision of statements regarding an investigation,” the unnamed Global Intelligence employee wrote. “Other prosecutors have reviewed this matter during other trial proceedings, finding this incident was more of a lost-in-translation issue as opposed to some sort of impropriety.”

WIRED requested the names of those prosecutors but did not receive a response.

No Receipts

The challenges in Ohio and Texas have hinged on an unusual aspect of Cybercheck that differentiates it from other digital forensics tools: The automated system doesn’t retain supporting evidence for its findings. As Mosher has testified under oath in multiple jurisdictions, Cybercheck doesn’t record where it sources its data, how it draws connections between various data points, or how it specifically calculates its accuracy rates.

In Mendoza’s case, for example, no one knows exactly how Cybercheck determined that the email address “ladypimpjuice625@aol.com” belonged to Mendoza. Nor did Global Intelligence explain exactly how the system determined that Mendoza’s cyber profile had pinged the wireless devices near 1228 Fifth Avenue.

Mosher has testified that the only information Cybercheck retains during its search process is the data it deems relevant to the investigation, all of which is included in the reports it automatically generates for investigators. Anything else, including potentially contradictory information about who owns a particular email address or online alias, is supposedly processed by the algorithms and used to calculate the accuracy scores that Cybercheck includes in its reports but isn’t archived.

“When you're asking, you know, do we preserve all the artifacts and all the data that we crawl—we couldn't realistically do that because it's zettabytes of data,” Mosher testified in the Texas Daubert hearing on January 19, 2024. A zettabyte is equivalent to more than 1 trillion gigabytes.

Mosher has testified that Cybercheck doesn’t need to show its work because its conclusions are derived from open source data that anyone with the proper open source intelligence (OSINT) training can find on the web.

“If you give that [Cybercheck] report to a skilled investigator that knows cyberspace and machine learning, they're going to come up with the exact same results,” Mosher testified during the murder trial of Adarus Black, in Summit County.

Rob Lee is an OSINT expert and chief of research and faculty lead at the SANS Institute, a leading provider of cybersecurity and infosec training. According to Mosher’s résumé and

court testimony, Mosher took more than a dozen SANS Institute training courses prior to founding Global Intelligence.

At WIRED's request, Lee and a team of researchers at the SANS Institute reviewed Cybercheck reports and the descriptions of the system that Mosher has given under oath. They say it's highly unlikely that some of the information in the reports can be gathered from publicly available sources.

Specifically, to determine when a particular device has pinged a wireless network, an analyst would need to either physically intercept the signal or have access to the device or the network's logs, neither of which are open source, Lee says. That kind of access requires a search warrant.

"There is a lack of peer review and transparency in [Cybercheck's] algorithmic processes, which makes me question the legitimacy, sufficiency, and legality of the datasets used for accurate profiling and geolocation," Lee tells WIRED. "The claim of achieving this level of accuracy using only open source data without further validation and transparency in the tool's methods and data sources is highly suspicious and questionable."

A Global Intelligence employee tells WIRED that law enforcement works with "industry analysts and experts in the open source intelligence space who are manually replicating and backstopping intelligence data from our reports." They add that "investigations and prosecutions only move ahead on the strength of the evidence gathered by agencies and verified after backstopping Cybercheck intelligence." The company's response did not address claims that certain data, such as whether a device connected to a specific Wi-Fi network, are typically not accessible via open source methods.

"Completely False"

During the Black murder trial in November 2022, Mosher testified that, since January 2021, Cybercheck had run approximately 1,900 searches for suspects' historical locations and another 1,000 searches for their real-time locations. Out of those 2,900 searches, Mosher testified, there was only one search in which the individual didn't turn out to be in the location Cybercheck listed for their cyber profile.

But in interviews with WIRED and in emails obtained by WIRED through public records requests, more than one of Cybercheck's law enforcement clients allege the company's technology provided information that investigators were unable to substantiate or that contradicted reliable sources.

In January, Mark Kollar, an assistant superintendent with the Ohio Bureau of Criminal Investigation (BCI), wrote an email to Cybercheck about a search warrant his agency had served to an email provider seeking information about an account that Cybercheck linked to a suspect. "The email provider is saying that the email listed in the Cybercheck report doesn't exist and has never existed," Kollar wrote.

The Ohio BCI, which is a division of the state attorney general's office, entered into a $30,000 trial contract with Cybercheck in August 2023 and submitted more than a dozen cases to the company, Steve Irwin, a spokesperson for the attorney general's office, tells WIRED. "BCI has not received results on many of the cases and some of the leads produced

haven't panned out," he says. "Due to the lack of investigative leads that have been produced, BCI has no intentions of entering into another contract with the company."

The Yakima County Sheriff's Office, in Washington, signed an $11,000 contract in 2022 allowing them to submit 20 cases to Cybercheck. "I think we still have access to Cybercheck, but we don't use it," Casey Schilperoort, the sheriff's public information officer, wrote in an email. "I heard that we don't receive much or accurate information."

In an unofficial email chain in which investigators from different agencies shared their experiences with the technology, which WIRED obtained through a public record request, Aurora, Colorado detective Nicholas Lesnansky wrote that Cybercheck had identified someone as a suspect in one of his department's homicide cases because the person's cyber profile pinged a router located at an address of interest. "Detectives went and spoke to the resident at that home who has lived there for 20+ years and never had a router by that name so we can't corroborate their information," Lesnansky wrote. Neither Mosher nor Global Intelligence responded to WIRED's inquiry about Lesnansky's claims.

In a second Aurora case involving the fatal shooting of a 13-year-old, Global Intelligence staff were "adamant" that Cybercheck had identified the killer, but Lesnansky's investigation was pointing toward an individual he considered a more likely suspect. "They then came up with a scenario where it was a gang initiation thing where the person they had identified was driving the person I think is more likely around," Lesnansky wrote. "I doubt the suspect Cybercheck identified and the other person I find more likely are driving around together as one has had his house shot up by the other several times."

On the same email chain, Heather Collins, a special victims unit intelligence analyst with the Mississippi Bureau of Investigation, wrote that she used Cybercheck on a missing juvenile case. "They gave us information on possible 'suspects' and it wound up being completely false. We located the missing juvenile using other methods. They wasted our time."

Mosher did not respond to WIRED's questions about Collins' allegation that the information Global Intelligence provided was false.

In other cases, Cybercheck appears to have produced accurate information, although investigators weren't always able to act on it.

Joe Moylan, the public information officer for the Aurora Police Department, says that his agency has requested information from Cybercheck on five cases, and that in two of those cases the technology was "beneficial to the investigations," although no arrests have been made as a result.

In 2017, then 9-year-old Kayla Unbehaun was abducted. For years, the South Elgin, Illinois police department searched for Unbehaun and her noncustodial mother, Heather Unbehaun, who was accused of the abduction, following her trail to Georgia, where they hit a dead end. During that time, the department signed a contract with Global Intelligence, and sergeant Dan Eichholz received a Cybercheck report that placed Unbehaun and her mother in Oregon, he tells WIRED. It was a new lead, but because Cybercheck didn't provide any evidence to support its findings, Eichholz couldn't use the report to obtain a search warrant.

Unbehaun was finally reunited with her father in 2023, after an employee at a consignment shop in Asheville, North Carolina, recognized her mother from a picture shown on the Netflix

show *Unsolved Mysteries*. After Unbehaun was located, Eichholz learned during the follow-up investigation that, until several months earlier, the pair had indeed been living in Oregon.

“I don’t want to say it wasn’t actionable, but I couldn’t just take their information and go with it,” Eichholz says. “That was always the hang-up for us. ‘OK, you got me this information, but I still have to check and verify and do my thing with search warrants.’” The child abduction case against Heather Unbehaun is ongoing.

Any Help They Can Get

Cybercheck has spread to law enforcement agencies across the country thanks to generous marketing offers and word-of-mouth recommendations. But in interviews with WIRED and the email exchanges we examined, there was little evidence that law enforcement agencies sought or received evidence to support Global Intelligence’s claims about what its technology could do.

Prosecutors who spoke to WIRED, such as Borden from Midland County, say they learned about Cybercheck because law enforcement in their jurisdiction had been using it. And when it came up in a case, they let the adversarial court system decide whether or not it was legitimate.

“It was new technology and I was curious, so I was like, ‘Let’s give it a try and see how far we can get,’” Borden says. “I’m thankful that it didn’t come into evidence in my case, that I didn’t need it to get my conviction.”

Emails show Global Intelligence sales representatives regularly offered to run police departments’ cases through Cybercheck for free in order to demonstrate the technology. They also referenced cases that Global Intelligence characterized as high profile and that Cybercheck supposedly helped solve, without naming the cases outright or providing evidence that Cybercheck had made any difference in the investigations.

Emails obtained by WIRED from the Ohio Bureau of Criminal Investigation show that investigators were initially excited to see what information Cybercheck could provide about their cold cases. They even introduced Global Intelligence sales representatives to other law enforcement agencies in Ohio. That enthusiasm seems to have helped convince other agencies to trust the company.

Gessner, from the Summit County Prosecutor’s office, says that when his agency was deciding whether to use Cybercheck evidence, it asked the Ohio BCI’s cybercrimes unit for an opinion. “They said, yes, it makes sense … we don't have the technology to do this, but we'd love to have it.” County prosecutors also reached out to the SANS Institute, he says, and were told the institute didn’t “do this type of stuff.”

But even as it has withdrawn evidence that Cybercheck provided, Gessner says the Summit County Prosecutor’s Office is asking other companies whether they can do the same kind of open source locating that Global Intelligence marketed.

“We don’t want to shut doors that can help point to the truth in our cases,” he says.