GREGORY, Circuit Judge, dissenting:

The Fourth Amendment exists to protect "'the privacies of life' against 'arbitrary power,'" *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)), and requires that law enforcement obtain a warrant prior to conducting a search, *id.* at 304 (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). In no uncertain terms, it states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

When officers violate these principles, the exclusionary rule, created by the Supreme Court to safeguard against Fourth Amendment violations, generally prohibits use of illegally obtained evidence to prove the defendant's guilt at trial. *United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014) (collecting cases). However, the exclusionary rule is not a "strict-liability regime," *Davis v. United States*, 564 U.S. 229, 240 (2011), and only applies where its application will "deter future Fourth Amendment violations," *id*. at 236–37; *see also Stephens*, 764 F.3d at 335; *Illinois v. Krull*, 480 U.S. 340, 347 (1987). Where an officer reasonably relies on a warrant later determined to lack probable cause, the good faith exception permits admission of the evidence despite the constitutional violation. *United States v. Leon*, 468 U.S. 897, 918–21 (1984). Whether evidence should be excluded or admitted following a Fourth Amendment violation requires us to assess if "a reasonably well[-]trained officer would have known that the search was illegal in light of all of the circumstances." *Herring v. United States*, 555 U.S. 135, 145 (2009) (internal quotation marks omitted).

To consider these important questions—whether there is a Fourth Amendment violation, and whether the *Leon* good faith exception should apply—requires courts to examine the underlying warrant and the circumstances pertaining to its issuance and execution. That task will sometimes require courts to wade through murky constitutional and doctrinal waters to provide necessary guidance to district courts, attorneys, law enforcement, and citizens alike. But our Court has decided not to do so here, opting instead to sidestep the complex issues presented in this case. The majority of this Court has decided to affirm the district court's opinion, but its reasoning is fractured.

I concur largely in the writings of Judge Wynn and Judge Berner in finding that there was a constitutional violation, as I believe that the geofence warrant at issue glaringly infringed on the Fourth Amendment. However, I write separately to explain why I believe the good faith exception is inapplicable in this case.

I.

Google account users can opt in to location history on their mobile devices, which allows users to keep track of locations they have visited. J.A. 127. At the time of the offense, Google processed and stored this location history if users shared it via location reporting. J.A. 125, 129–30. Pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, law enforcement can obtain legal process compelling Google to disclose location information, including through geofence warrants. J.A. 124–25. In conjunction with the Department of Justice, Google developed a three-step anonymization and narrowing protocol in response to these geofence requests. J.A. 1344.

In this case, Detective Hylton swore an affidavit for a geofence warrant for Google users' location history. J.A. 107. The warrant, at Step One, authorized a search for anonymized data of Google users with shared location history for a limited time frame (one hour) and a small geographic scope (150-meter radius) where the crime occurred. *See* J.A. 107, 110–11. At Step Two, it authorized a search expanded in both time (one more hour in total) and geographic scope (completely unbounded) and narrowed to a subset of users. J.A. 110–11, 135–36.[1] And at Step Three, the search included non-anonymized, identifying information for a smaller subset. J.A. 111.

Significantly, the warrant did not explain how law enforcement would narrow the list of users at Steps Two and Three based on the information obtained at Step One. *See* J.A. 110–11. Even now, the government cannot tell us what justified the more intrusive searches at Steps Two and Three, or how or why there was probable cause to search those individuals. *See e.g.*, Oral Argument at 57:17, 1:10:11. Instead, the warrant gave law enforcement broad discretion to request and obtain a seemingly unlimited amount of data associated with devices identified at Step One, checked only by Google.

At Step One, Google provided anonymized data for nineteen devices located within the geofence—which included homes, a hotel, a large church, and a restaurant—thirty minutes before and after the robbery. J.A. 1354, 1357. At Step Two, Detective Hylton

[1] Chatrie argues that the data provided at Step Two could be considered non-anonymized, as an expert could identify each of the nine users based on the data provided, such as where they traveled during the expanded location and time. Oral Argument at 1:37:48, *United States v. Okello Chatrie*, (4th Cir. 2025) (No. 22-4489), https://www.ca4.uscourts.gov/OAarchive/mp3/22-4489-20250130.mp3 (henceforth "Oral Argument).

ultimately identified nine devices and requested additional location data for those devices expanded for thirty minutes before and thirty minutes after the one-hour window authorized at Step One, and without any geographic limitations. J.A. 1355. This production allowed Detective Hylton to track those devices outside of the confines of the geofence for an hour before and after the crime was committed. At Step Three, Detective Hylton requested, and Google provided identifying information about the accounts associated with three of the devices identified at Step Two. J.A. 1355–56. Consequently, the warrant permitted Detective Hylton to obtain information that the Constitution forbids without probable cause—the detailed movements of anyone with a device identified at Step One—without any additional judiciary oversight. Such lack of additional judiciary oversight was an error by the magistrate.

But that is not enough. As we know from *Leon*, the magistrate's errors alone are insufficient to warrant suppression of evidence obtained pursuant to a deficient warrant. This is because magistrates are "neutral judicial officers" who have "no stake in the outcome of particular criminal prosecutions." *Leon*, 468 U.S. at 917. As such, excluding evidence because of a magistrate's error would not deter similar misconduct and may even discourage an officer in the future. *Id*. at 920 (stating that excluding evidence obtained following an officer's objectively reasonable reliance on a search warrant would "in no way affect his future conduct unless it is to make him less willing to do his duty.") (citation and quotation marks omitted).

"Deference to the magistrate, however, is not boundless." *Id*. at 914. Reliance on the warrant alone is therefore insufficient to protect against exclusion of the recovered evidence.

Such is the case where the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Id*. at 923. The good faith exception also does not apply where the facts indicate that the investigating officer "could not have harbored an objectively reasonable belief in the existence of probable cause." *Id*. at 926. As one of my colleagues concluded in assessing the Fourth Amendment violation in this case, *see* Berner, J., concurring at 109–13 the warrant in this case lacked probable cause. As I will now explain further, the evidence in this case should have been excluded, as "it is clear that . . . the officer [had] no reasonable grounds for believing that the warrant was properly issued." *Leon*, 468 U.S. at 922–23.

To begin, neither the affidavit nor the warrant explained how law enforcement would conduct its review between the various steps of Google's process. J.A. 107, 110–11. Nevertheless, the warrant authorized Detective Hylton to obtain information at Step Three that was of the most personal nature—account-identifying information—for any account associated with a device he identified from Step One without probable cause for each individual's data. But for what amounted to a general warrant, Detective Hylton would not have otherwise received such information.

Additionally, Detective Hylton had unbridled discretion to determine who would be subject to intrusive and expansive searches. For example, at Step Two, Detective Hylton initially requested additional location data for all nineteen users identified at Step One, expanded for thirty minutes before and thirty minutes after the originally requested one hour window, and without any geographic limitations. J.A. 1354–55; *see also* J.A. 98. His email to Google stated that he was requesting the additional data "in an effort to rule out

possible co-conspirators," and that nine of the users "may fit the more likely profile of parties involved." J.A. 98. At oral argument, the government contended that it was looking for witnesses as well. *See* Oral Argument at 53:51. Detective Hylton followed up on his email twice on the two following days. J.A. 100, 1059. He then left two voicemails for a Google specialist; the specialist returned his call and recounted the issues in Detective Hylton's email, describing how his request did not follow the three-step process and explaining the importance of narrowing his request. J.A. 102, 1584–85. The next day, Detective Hylton sent an email narrowing his request to nine users. J.A. 102, 1059, 1584. Google provided Detective Hylton the anonymized, expanded data for nine users. J.A. 1585. As was explained before, the government cannot explain how or why Detective Hylton narrowed in on the particular users. And at no point during this process did Detective Hylton seek judicial intervention, although the warrant did not contain sufficient probable cause and particularity to authorize these additional searches.

Detective Hylton could not have reasonably believed that the liberty authorized by the warrant was constitutional given the lack of specificity the Fourth Amendment explicitly demands.[2] *United States v. Groh*, 540 U.S. 551, 563 (2004) (citing *Harlow v. Fitzgerald*, 457 U.S. 800, 818–19 (1982)) ("Given that the particularity requirement is set forth in the test of the Constitution, no reasonable officer could believe that a warrant that

[2] *See, e.g.*, *Groh v. Ramirez*, 540 U.S. 551 (2004) (declining to extend the *Leon* good faith exception to law enforcement officials who issued a warrant that listed only the location of the evidence without describing the items to be seized); *United States v. George*, 975 F.2d 72 (2d Cir. 1992) (declining to extend the good faith exception to a warrant issued following a robbery that included only a list of items, the address subject to search, and the phrase "any other evidence relating to the commission of a crime).

plainly did not comply with that requirement was valid."). On its face, the warrant lacked the requisite constitutional requirements to conduct increasingly intrusive searches at Steps Two and Three of Google's process. Instead, the warrant ceded authority and decision-making from an independent judicial officer to a private corporation. No reasonable officer could believe that execution of this geofence warrant in this manner comports with the Fourth Amendment and the liberties it serves to protect. In the same way that this cannot cure the constitutional violation that occurred, *see* Wynn, J. concurring at 35–53 and Berner, J., concurring at 109–13, it does not excuse the officer's indiscretions. Exclusion of the evidence is therefore appropriate here.

One dear colleague suggests that even if there was a search, placing restraints on law enforcement's use of geofence location data and other emerging technologies is unjustified. Wilkinson, J., concurring at 22–23 (stating "[e]ven if there was a search, there is no room for emergent judicial hostility" because such restraint would "frustrate law enforcement's ability to keep pace with tech-savvy criminals" and "[m]ore cold cases would go unsolved"). I am not unmindful of nor insensitive to the number of cases that go unsolved each year and the lack of closure that results from this unfortunate reality. I am, however, vehemently opposed to the notion that new technology erodes the protections and principles of our Constitution. Crimes have gone unsolved due to lack of suspect and witness identification, lack of evidence, and other issues beyond law enforcement control presumably since the beginning of recorded time.

That fact, however, has never justified infringement on the Constitution and as such, should not be used as a reason to withhold Fourth Amendment protections or excuse Fourth

Amendment violations. Indeed, the Supreme Court has said as much. Specifically, the Supreme Court stated "that [t]he efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great [constitutional] principles." *Mapp v. Ohio*, 367 U.S. 643, 648 (1961) (quoting *Weeks v. United States*, 232 U.S. 383, 391–92 (1914)). Simply put, the judiciary may not be a safe harbor to violations of the Fourth Amendment because cold cases—which have always been an unfortunate reality—will continue. This must remain true no matter how well-meaning the investigative officers' intentions. And technological developments nor corporate practices should alter that calculus.

Some of my colleagues suggest that exclusion is not warranted in this case because this Court nor any other court had opined on the validity of geofence warrants at the time of Detective Hylton's application. Thus, they suggest that any error on Detective Hylton's part resulted from the lack of clear direction regarding geofence warrants. But, contrary to that suggestion, an officer need not know the judiciary's view on the use of new technology with the Fourth Amendment to know that the information in the warrant was insufficient. It is well-settled that, to be valid, a warrant must include the particular person, place, or thing to be searched. *Smith*, 442 U.S. at 736 n.2 (citing U.S. Const. amend. IV). Accordingly, whatever the alleged uncertainty regarding geofence warrants, it was not unclear what the Constitution demands of all warrants. That being the case, the lack of authority regarding geofence warrants does not end the inquiry into the objective reasonableness of Detective Hylton's conduct. And for good reason, as endorsement of that practice would run the risk of forgiving law enforcement impropriety simply because

no court has specifically forbidden it. That is the very type of behavior the Supreme Court cautioned against in the context of retroactivity of Fourth Amendment rulings. Namely, that "police or other courts [would] disregard the plain purport of our decisions and [] adopt a let's-wait-until-it's-decided approach." *Leon*, 468 U.S. at 912 n.9 (citing *U.S. v. Johnson*, 457 U.S. 537, 561 (1982)) (internal quotation marks omitted). If we permitted that course of action, Fourth Amendment protections would become a nullity in the face of rapidly emerging technology.

The same unfortunate fate would result if Detective Hylton's belief in his actions was dispositive. *Leon* instructs us to assess whether the investigating officer held an objectively reasonable belief in the warrant's validity and his actions. 468 U.S. at 919. Detective Hylton's subjective belief, or what he "could have" believed, then, is therefore of little moment. *Contra* Heytens, J., concurring at 88 (stating "because the investigating officer *could have had* 'an objectively reasonable good-faith belief that his conduct was lawful,' I think the district court was right to withhold 'the harsh sanction of exclusion'") (citing *Davis*, 564 U.S. at 238, 240) (emphasis added) (internal brackets omitted).

This too makes sense as constitutional rights should not be so subjugated to the will of individual officers. *Leon*, 468 U.S. at 915 n.13 ("Good faith on the part of the arresting officers is not enough") (citing *Henry v. United States*, 361 U.S. 98, 102 (1959)) (internal brackets and quotation marks omitted). If subjective good faith alone were the test, the protections of the Fourth Amendment would evaporate, and the people would be "'secure in their persons, houses, papers, and effects,' only in the discretion of the police." *Id*.

Similarly, it is a perilous day when our Fourth Amendment protections lie in the hands of a private company, and constitutional rights should not and cannot be defined by the internal policies of a private corporation. This is so even where the process was created with input from law enforcement. To that point, I note that the government and some of my colleagues highlight that Google's process was created in conjunction with the Department of Justice. Notably, the government's interest in defining the Fourth Amendment right is no greater than that of the defense counsel, other attorneys, and the public at large—none of whom were offered a seat at the table. And, even if Google had opened the forum to all potential stakeholders, its process would still lack finality because corporations lack the authority to interpret the Constitution. That responsibility belongs to the courts, and we must not relinquish it to those not charged with protecting the Constitution or otherwise abdicate it because the task seems too difficult.

II.

Law enforcement should not be denied the benefit of the efficiencies that emerging technologies offer. However, when seeking digital evidence, officers must demonstrate at least the same level of supporting information necessary to justify the search of physical places and things. In other words, officers should not be permitted, with aid of an unbridled warrant, to shake the proverbial digital tree without an objectively reasonable belief that the warrant and the manner of its execution are consistent with the Fourth Amendment. And that reasonable belief must be founded on something more than the commonality of

the technology at issue in the case. This is especially so given that technology has and continues to shift our understanding of "person, place, or thing."

Some cry "novelty" and "technological change" as an excuse for a fundamental departure from our constitutional principles. But one thing is for certain: technology will continue to shift, but the basic protections of the Fourth Amendment must remain. The people's rights against unreasonable searches and seizures cannot not bend to accommodate the volatility of technology. Rather, new technologies must bend to accomplish the vitality of the protections guaranteed to the people under the Fourth Amendment. Regrettably, the ever-increasing extension of the good faith exception to the exclusionary rule has turned this sacred principle of Fourth Amendment interpretation on its head.

The Constitution nor Fourth Amendment precedent to date anticipated that person may one day refer to a non-human, such as Optimus; places could encompass locations in the Metaverse (or otherwise only digitally accessible); and things could include intangible objects that exist only electronically. Given that reality, the judiciary still must fulfill its role and duty to ensure that the interpretation of the Constitution does not fall solely in the hands of anyone not charged with protecting the rights it guarantees. Our Court failed to do so here. Thus, I must dissent.