

ADVOCATE

NEWSLETTER FOR THE DEFENSE
Fall 2025

The Editors' Message

Despite the stress of continuing budget constraints and negotiations, we are impressed at the level of dedication the lawyers in our district demonstrate on a daily basis. The defendants in our district are truly fortunate to have attorneys that persevere in providing quality representation in these uncertain times.

To support your practice, this issue of the *Zealous Advocate* offers a multitude of articles covering current issues in federal criminal defense. Inside, you will find articles on Fourth Amendment issues, including geofence warrants, terms of service in digital spaces, and privacy implications of drone surveillance. Other topics include a ransomware primer and the use of textualism in statutory interpretation. For those going to trial with experts, there are articles on the confrontation clause as well as *Diaz's* effect on expert testimony. And, for cases going to sentencing, you will find articles about using Chapter 1 of the sentencing guidelines to your client's advantage, the Vulnerable Victim adjustment, and an update on Amendment 821 and status points. Finally, we have legal updates, which include new federal rules and guidelines.

As always, we hope you find these articles helpful to your practice. This publication is one of several ways we endeavor to keep defense attorneys in our district up to speed on recent legal developments. We also provide CLE training programs for attorneys in our district, with the next one taking place in person this fall at the Beaufort Hotel in Beaufort, North Carolina. We look forward to seeing everyone at our next seminar and hope you know how important your work is for criminal defendants in the EDNC.

Vidalia Patterson & Laura Wasco
ZA Editors



Inside the Fall 2025 Issue

PANEL ATTORNEY INFORMATION....2

PRACTICE TIPS

<i>Geofence Warrants</i>	2
<i>Terms of Service & Fourth Amendment</i>	4
<i>Defending Privacy in the Age of Drones</i>	5
<i>Ransomware Primer</i>	6
<i>Textualism as a Tool</i>	8
<i>Experts—Confrontation Clause</i>	9
<i>Expert Testimony on Classwide Mental States</i>	10
<i>Chapter One Guidelines</i>	13
<i>Fighting the Vulnerable Victim Label</i>	14
<i>Status Points—Amendment 821 and Barrett</i> ...	15

LEGAL UPDATES

<i>4th Circuit Update</i>	16
<i>U.S. Supreme Court Update</i>	17
<i>Amended Rules and Guidelines Update</i>	17

LOCAL NEWS..... 19

THE ZEALOUS ADVOCATE

Office of the Federal Public Defender
For the Eastern District of North Carolina
150 Fayetteville Street, Suite 450
Raleigh, NC 27601
Tel: (919) 856-4236
Fax: (919) 856-4477

G. Alan DuBois, Federal Public Defender

April Bunn, Panel Administrator

Vidalia Patterson, Co-Editor, vidalia_patterson@fd.org

Laura S. Wasco, Co-Editor & Layout, laura_wasco@fd.org

Gloria Gould & Melanie Fisher, Design & Layout

PANEL ATTORNEY INFORMATION

Reminders

Please watch for emails our Panel Administrator, April Bunn, sends out regarding any training, CLE opportunities, and new procedures and protocols regarding eVoucher and updates. You can always find the most updated version of the Attorney Manual for eVoucher on the Court's website: <http://www.nced.uscourts.gov/pdfs/AttorneyManual.pdf>

Seminar BOLOs

Registration is closed for our Fall 2025 Federal Criminal Practice Seminar, which will take place Thursday October 23rd through Friday October 24th at the Beaufort Hotel in Beaufort, North Carolina.

Please be on the lookout for information about our only seminar next year, tentatively set for November 2026. Additional details, including registration and reservation information, will be sent out later and will also be posted to our website.



PRACTICE TIPS

Courts, Corporations, and Cold Cases: The Constitutionality of Geofence Warrants

Geofence warrants are a modern tool used by law enforcement to obtain individuals' cell phone location data from service providers. Google, the most common recipient of such warrants, has developed a three-step process that law enforcement may use to request user location data within a specific location and time period.¹ As use of this tool has rapidly expanded,² defendants have raised Fourth Amendment challenges,³ often relying on the Supreme Court's landmark Fourth Amendment case *Carpenter v. United States*.⁴ The Fourth Circuit's recent *en banc* decision in *United States v. Chatrie*⁵ firmly entrenches a circuit split on geofence warrant constitutionality.⁶ In a one-line decision, the Fourth Circuit affirmed the district court's judgment denying Chatrie's motion to suppress location data obtained by a geofence warrant.⁷ However, the rehearing produced seven concurrences and one dissent, with conflicting conclusions and rationales. This article analyzes some of these opinions to identify pathways for future Fourth Amendment challenges to geofence warrants.

Chatrie arose out of a Virginia bank robbery. Traditional investigation failed to locate the robber, but a detective saw the suspect using a cell

phone on bank security footage.⁸ The detective obtained a geofence warrant for all location data within a 150-meter radius around the bank for 30 minutes before and after the robbery.⁹ Working through Google's three-step process, the detective first requested pseudonymized data for all users, ultimately 19 individuals, within this time range and location.¹⁰ Next, the detective reviewed the data and requested two hours of still-pseudonymized data from a wider area for nine of the 19 users.¹¹ Finally, the detective requested identifying information for three of the nine accounts.¹² This information led law enforcement to Chatrie, who was arrested and prosecuted.

Initially, the district court held that the geofence warrant lacked particularized probable cause, but found that the good-faith exception to the exclusionary rule applied, noting the dearth of case law on geofence warrants at the time of the investigation.¹³ On appeal, a three-judge panel of the Fourth Circuit affirmed over Judge Wynn's dissent, holding that the third-party doctrine applied because Chatrie voluntarily shared his location information with Google and thus no Fourth Amendment search occurred.¹⁴

The Fourth Circuit's *en banc* rehearing resulted in divergent opinions on nearly every Fourth Amendment issue discussed. Most opinions relied heavily on the Supreme Court's analysis in *Carpenter*, where the Court found a reasonable expectation of privacy in seven days of cell-site location information and refused to extend the third-party doctrine to cover such information.¹⁵ Beyond applying that framework, however, there was little agreement.

Chief Judge Diaz concurred, but solely on the district court's application of the good-faith exception, emphasizing the geofence warrant's approval by a neutral magistrate.¹⁶ Chief Judge Diaz also cautioned against "sweeping constitutional pronouncements," but indicated that the good-faith exception may not continue to "carry the day."¹⁷

Judge Richardson would have gone further to hold that obtaining two hours of location information was not a Fourth Amendment search.¹⁸ Finding that the third-party doctrine squarely governed the case, Judge Richardson reasoned that Chatrie voluntarily exposed the information to Google by opting in to location sharing, and the information obtained was far less revealing than that in *Carpenter*.¹⁹ He emphasized the voluntary nature of the opt-in process and the user's "ultimate control" over his data.²⁰

Judge Wilkinson agreed that no search had occurred and provided additional policy considerations in support of geofence warrants.²¹ He reasoned that disabling geofence warrants would undermine legitimate law enforcement and allow tech-savvy criminals to evade detection, resulting in more cold cases.²² He also worried that prohibiting the practice would hamper public-private cooperation and stifle data sharing between law enforcement and companies like Google.²³ Final-

ly, Judge Wilkinson cautioned against applying the exclusionary rule in a way that would preempt legislative input in this rapidly evolving area.²⁴

In contrast, Judge Wynn would have held that police conducted a Fourth Amendment search.²⁵ After extensively cataloguing relevant Fourth Amendment cases,²⁶ Judge Wynn turned to the *Carpenter* factors – the data’s comprehensiveness, retrospective nature, intimacy, and ease of access – and found they applied with equal or greater force, concluding the search invaded Chatrle’s reasonable expectation of privacy.²⁷ Judge Wynn rejected a straightforward application of the third-party doctrine, emphasizing the revealing nature of location history and reasoning that opting in was not meaningfully voluntary.²⁸

Judge Berner, reaching a similar but narrower conclusion, would have held that the step one request was not a Fourth Amendment search but that steps two and three were.²⁹ Specifically, Judge Berner would have held that individuals have a reasonable expectation of privacy in non-anonymous location data.³⁰ Analyzing probable cause at the time the geofence warrant was issued, she reasoned, the government would have been unable to provide facts to support conducting a search targeting the individuals whose data was obtained at step two.³¹ Rather, with judicial authorization preceding only step one, Google “was the sole entity that could confine the scope of the ultimate search,” but “probable cause determinations cannot be delegated to private entities.”³²

The Fourth Circuit’s widely divergent views on geofence warrant constitutionality indicate the issue is not resolved. However, the opinions suggest viable pathways for future Fourth Amendment challenges. Defense attorneys should continue to distinguish straightforward applications of the third-party doctrine. Extensive trial testimony from *Chatrle* establishes the near-automatic ease of opting in to location sharing and the difficulty in regaining control of this data.³³ Likewise, *Carpenter* continues to provide a blueprint for Fourth Amendment challenges to geofences, as evidenced by its pervasive presence in *Chatrle*. Furthermore, the opinions suggest probable cause and particularity challenges remain viable. Steps two and three of Google’s process, specifically, displace the neutral magistrate role and provide significant law enforcement discretion to obtain additional personal information not specified in the original warrant. After *Chatrle*, courts may be less willing to provide Google and law enforcement with unfettered discretion to expand parameters after step one to obtain non-anonymous user data. Finally, as courts produce additional decisions and extensive writing on geofence warrant constitutionality, the good-faith exception may become increasingly difficult to invoke. As Chief Judge Diaz reaffirms, the good-faith exception “may not carry the day in the future.”³⁴

¹ See generally Barbara Bathke, Comment, *Google and the Role of Surveillance Intermediaries in Geofence Warrants*, 26 Tul. J. Tech. & Intell. Prop. 111 (2024) (discussing Google’s role as a provider of user location data to law enforcement).

² See Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of All US Demands*, TechCrunch (Aug. 19, 2021), <https://techcrunch.com/2021/08/19/google-geofence-warrants/> (last visited July 15, 2025).

³ See, e.g., *In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); *Tomanek v. State*, 314 A.3d 730 (Md. App. Ct. 2024).

⁴ *Carpenter v. United States*, 585 U.S. 296 (2018) (holding that an individual maintains a reasonable expectation of privacy in seven days of cell-site location information and refusing to extend the third-party doctrine to such information).

⁵ *United States v. Chatrle*, 136 F.4th 100 (4th Cir. 2025) (per curiam).

⁶ The Fifth Circuit, recently deciding one such challenge, held “that geofence warrants are general warrants categorically prohibited by the Fourth Amendment.” *United States v. Smith*, 110 F.4th 817, 838 (5th Cir. 2024).

⁷ *Chatrle*, 136 F.4th at 100; see also *United States v. Chatrle*, 590 F. Supp. 3d 901, 941 (E.D. Va. 2022).

⁸ See *Chatrle*, 136 F.4th at 144 (Berner, J., concurring).

⁹ *Id.* at 145.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.* at 145-46.

¹³ See *Chatrle*, 590 F. Supp. 3d at 929, 937-38.

¹⁴ *Chatrle*, 107 F.4th 319, 332 (4th Cir. 2024) (citing *United States v. Miller*, 425 U.S. 435, 443 (1976); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)). Under the third-party doctrine, when an individual knowingly and voluntarily shares information with a third party, he loses any reasonable expectation of privacy in that information.

¹⁵ *Carpenter*, 585 U.S. at 310, 315-16. The Court, in finding a reasonable expectation of privacy, emphasized the information’s comprehensiveness, retrospective quality, intimate nature, and law enforcement’s ease of acquisition. See *id.* at 310-13. In refusing to extend the third-party doctrine, the Court pointed to the information’s revealing nature and doubted whether sharing was meaningfully voluntary. See *id.* at 314-15.

¹⁶ See *Chatrle*, 136 F.4th at 103-04 (Diaz, C.J., concurring).

¹⁷ See *id.* at 109 (quoting *Chatrle*, 590 F. Supp. 3d at 941).

¹⁸ *Id.* at 130 (Richardson, J., concurring).

¹⁹ See *id.* at 139-41.

²⁰ See *id.* at 140 (“If Google compiles a record of his whereabouts, it is only because he has authorized Google to do so.”).

²¹ See *id.* at 109-10 (Wilkinson, J., concurring).

²² See *id.* at 110 (“Taking this tool of last resort out of law enforcement’s hands would leave these case files collecting dust.”)

²³ See *id.* at 111.

²⁴ See *id.* at 111-12 (“This type of compromise is a classic legislative task.”).

²⁵ *Id.* at 115 (Wynn, J., concurring).

²⁶ See *id.* at 116-20.

²⁷ See *id.* at 121-25.

²⁸ See *id.* at 126-29 (“[A] user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting ‘YES, I’M IN’ at midnight while setting up Google Assistant.” (quoting *Chatrle*, 590 F. Supp. 3d at 936)).

²⁹ *Id.* at 144 (Berner, J., concurring).

³⁰ *Id.*

³¹ *Id.* at 153.

³² *Id.* at 155 (citing *Birchfield v. North Dakota*, 579 U.S.

438, 469 (2016); *United States v. Rubio*, 727 F.2d 786, 794-95 (9th Cir. 1983)).

³³ See, e.g., *Chatrie*, 590 F. Supp. 3d at 910-14 (describing location data opt-in and deletion processes and accompanying user confusion); see also *Chatrie*, 136 F.4th at 128 (Wynn, J., concurring) (“Approving a lucrative location-tracking feature on a smartphone is frictionless by design.”).

³⁴ *Chatrie*, 136 F.4th at 109 (Diaz, C.J., concurring) (quoting *Chatrie*, 590 F. Supp. 3d at 941).

The ZA Editors thank Luke Pomrenke for contributing this helpful information. Luke was a third-year law student at the University of Michigan Law School and an intern in the FPD office during the Summer of 2025.



Terms of Service Don't Silence the Fourth Amendment

The internet—and technology, more broadly—is involved in just about everything we do. Chief Justice Roberts wisely stated that modern smartphones are “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”¹ With this internet usage comes the pervasiveness of terms of service (“TOS”). TOS agreements are the rules a person must agree to use a service and are generally legally binding.² Most, if not all, internet service providers (“ISP”) and websites that store user data have TOS, including social networking sites.³ The top five websites in the world all have TOS, with a combined monthly visit total of over 2 billion.⁴ It is safe to say that the average American interacts with an internet provider or website governed by TOS daily.

There have long been concerns in the legal community and the broader American public about the effect of the rise of digital technology on Fourth Amendment protection.⁵ While the Supreme Court’s holdings in *Riley v. California*⁶ and *Carpenter v. United States*⁷ indicate that Fourth Amendment rights entirely apply to digital data, the Court has never confronted how the TOS on a website can affect a user’s Fourth Amendment Rights. Renowned Fourth Amendment Scholar Orin S. Kerr recently discussed this issue in his January 2024 article *Terms of Service and Fourth Amendment Rights*.⁸ He found that the majority of courts that decided the issue held that TOS could restrict or even eliminate Fourth Amendment rights, but he argued persuasively against this holding.⁹ In this article, I will present the courts’ opinions on this issue and Kerr’s argument for why TOS do not alter an individual’s Fourth Amendment right. I will contribute to this discussion by presenting current jurisprudence in this area in the Fourth Circuit specifically.

Courts that have held that TOS can limit Fourth Amendment rights rationalize that agreeing to TOS can waive these rights or show there is

no reasonable expectation of privacy for the data governed by the TOS. For example, the Seventh Circuit held, in *United States v. Adkinson*, that T-Mobile’s provision of cell phone location records to the FBI did not violate the Fourth Amendment, in part, because its terms of service allowed T-Mobile to disclose user’s private information “[t]o protect [T-Mobile’s] rights or interests, property or safety or that of others.”¹⁰ The court said that the defendant signing up for a T-Mobile account created consent in advance to search “as a condition of receiving contracted services.”¹¹ Kerr notes many similar cases in which an ISP’s broad TOS prohibiting unlawful acts and allowing it to take action to enforce TOS is used as one argument for why a defendant did not have Fourth Amendment protections to data on the platform.¹²

In the Fourth Circuit to date, only one district court has ruled on the issue of TOS’s effect on Fourth Amendment protections. In *United States v. Lowers*,¹³ Judge Richard E. Myers II held, as one of several rationales to deny a motion to suppress, that the defendant did not have a reasonable expectation of privacy for child pornography stored in his Google account. Judge Myers noted, “Google users must agree that they will not use Google’s services to upload any child pornography, and Google’s privacy policy informs its users that Google may monitor user activity to detect illegal content.”¹⁴ Thus, he concluded that a reasonable person would not have expected files with prohibited content in them to be private.¹⁵ In this way, Judge Myers explicitly linked the existence of Google’s TOS to whether Lowers had a reasonable expectation of privacy for purposes of the Fourth Amendment. Since Google is allowed to monitor the defendant’s account according to the TOS, he had no reasonable expectation of privacy from the government in the account.

However, Kerr disagrees. He argues that TOS do not affect Fourth Amendment Rights because they are private owner-user agreements, which give rights to use another’s property, rather than agreements with the government.¹⁶ It is clearer that owner-user agreements do not alter Fourth Amendment rights when looking at Fourth Amendment cases involving these contracts in physical spaces.¹⁷ For example, in *Byrd v. United States*,¹⁸ the government argued that the defendant, Byrd, did not have Fourth Amendment Rights in the rental car he was driving because he was not an authorized driver according to the owner-user agreement. However, the Supreme Court rejected that argument, saying the purpose of the contract was simply to allocate risk between private parties, which is a different inquiry than whether Byrd had a reasonable expectation of privacy in the car when he was pulled over.¹⁹

According to Kerr, courts that reached the opposite conclusion about TOS and Fourth Amendment rights did so by incorrectly analo-

gizing them to cases of shared government spaces.²⁰ Shared government spaces are exceptions in which agreements (particularly workplace privacy policies) can alter Fourth Amendment rights, according to the Supreme Court plurality in *O'Connor v. Ortega*.²¹ For example, *Adkinson*²² cited *Medlock v. Trustees of Indiana University*²³ for the proposition that one could consent in advance to decreased Fourth Amendment rights to receive private contracted services but ignored that that case involved inspection policies at a public university.

Courts that have held that TOS do not limit Fourth Amendment rights generally adopt reasoning like Kerr's. They conclude that TOS do not reduce one's expectation of privacy. One prominent decision holding that TOS do not affect Fourth Amendment rights is the Sixth Circuit's *United States v. Warshak* ("Warshak III").²⁴ There, the court held a warrant was required to compel the contents of an email from an email provider.²⁵ In doing so, the court explained that the provider's TOS that it "may access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service" did not affect the Fourth Amendment protection of the emails.²⁶ The court reasoned that rights-holders frequently retained rights despite third-party access, like when renting a hotel room.²⁷ This proposition, the court said, must apply to new technology.²⁸ The court analogized that as the defendant in the seminal *Katz v. United States*²⁹ was held to have a reasonable expectation of privacy against the government during his phone booth call, despite the phone company having a contractual right to tap his call,³⁰ so too should a user of an ISP's service, even if its TOS gives the ISP access to user data.³¹

Although most courts that have ruled on the issue, including the only court within the Fourth Circuit, have held that TOS can reduce or even eliminate Fourth Amendment rights, Orin Kerr presents a strong argument that TOS do not affect these rights because they only govern the conduct of private parties. Given the nascency of jurisprudence in this area and the ubiquity of internet usage, this argument is essential to keep in mind anytime the government seeks access to a client's internet data without a warrant. If other possible relevant justifications for the search, like private search doctrine, do not apply, then this argument certainly should be raised. I recommend reading the entirety of Kerr's convincing article to gain a better understanding.

¹ *Riley v. California*, 573 U.S. 373, 385 (2014).

² *Terms of Service*, PC Mag, <https://www.pcmag.com/encyclopedia/term/terms-of-service> (last visited Apr. 10, 2025).

³ *Id.*

⁴ See *Top Websites in Worldwide (All Industries)*, Semrush, <https://www.semrush.com/trending-websites/global/all> (compiling data on the most visited websites) (last visited Apr. 10, 2025).

⁵ See, e.g., *United States v. Jones*, 565 U.S. 400, 417 (suggesting the Court reconsider Fourth Amendment doctrine considering the vast amounts of information available on people in the digital age.) (Sotomayor, J., Concurring).

⁶ 573 U.S. 373, 401 (2014) (holding that a warrantless search of a cell phone was unlawful).

⁷ 585 U.S. 296, 316 (2018) (holding that accessing cell-site location data generally requires a warrant).

⁸ 172 U. Pa. L. R. 287 (2024).

⁹ *Id.* at 289.

¹⁰ 916 F.3d 605, 608, 610 (7th Cir. 2019).

¹¹ *Id.*

¹² Kerr, *supra* note 8, at 298-99.

¹³ 715 F.3d 741, 754 (E.D.N.C. 2024).

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ Kerr, *supra* note 8, at 304.

¹⁷ *Id.* at 308.

¹⁸ 138 S. Ct. 1518 (2018).

¹⁹ *Id.* at 1528-1529.

²⁰ Kerr, *supra* note 8 at 313.

²¹ *Id.* 314-315 (citing 480 U.S. 709, 717-718 (1987) (O'Connor, J., plurality opinion)).

²² 916 F.3d at 610.

²³ 738 F.3d 867, 872 (7th Cir. 2013).

²⁴ 631 F.3d 266 (6th Cir. 2010).

²⁵ *Id.*

²⁶ *Id.* at 286-287.

²⁷ *Id.* at 285.

²⁸ See *Id.* ("The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

²⁹ 389 U.S. 347 (1967).

³⁰ *Smith v. Maryland*, 442 U.S. 735, 746-47 (1979) (Stewart, J., dissenting).

³¹ See *Warshak III*, 631 F.3d at 286 ("If we accept that an email is analogous to a letter or a phone call, ... the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment.").

The ZA Editors thank Tyler Wiesman for contributing this helpful information. Tyler was a third-year law student at Duke University School of Law and was an extern in the FPD office during the Spring of 2025.



Defending Privacy in the Age of Drones

The Fourth Amendment safeguards individuals from unreasonable searches and seizures, ensuring that "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated." *Olmstead v. United States*, 277 U.S. 438, 457 (1928). Over time, Fourth Amendment jurisprudence has evolved from a strictly trespass-based interpretation into a more privacy-centered approach. This was evidenced in *Katz v. United States*, which established that the Fourth Amendment applies

whenever and wherever an individual has a “reasonable expectation of privacy.” 389 U.S. 347, 360 (1967). Consequently, defining the bounds of “reasonable expectation of privacy” has presented itself with challenges, especially in the modern era of rapidly evolving technology. However, what remains true is the principle that what an individual seeks to keep private—even in a space accessible to the public—may receive constitutional protections. *Id.* at 352. As technology continues to evolve, questions arise about whether this privacy expectation extends into the airspace above us. This tension becomes particularly salient as courts confront the implications of drone technology, which allows for persistent, low-altitude surveillance.

The Court has generally upheld warrantless aerial surveillance under the Fourth Amendment when observations are made from lawful public airspace. In *California v. Ciraolo*, the Court held that warrantless aerial surveillance of an individual’s backyard at an altitude of 1,000 feet did not violate the Fourth Amendment because the observations were made from a public airspace where anyone could legally fly. 476 U.S. 207, 215 (1986). Similarly, in *Florida v. Riley*, law enforcement’s use of a helicopter flying at 400 feet to view a greenhouse was deemed constitutional under the same reasoning. 488 U.S. 445, 450 (1989). Both *Ciraolo* and *Riley* rest on the notion that any member of the public could have legally flown in the airspace at these altitudes and could have captured the same views. Thus, these cases have been grounded in the core that, if the public can see it, then law enforcement legally can too, interpreting the Fourth Amendment in the realm of aerial surveillance through the lens of the public vantage point. However, the rapid rise of drone technology may challenge this framework.

Today we see the use of drone technology becoming increasingly integrated into law enforcement investigations. Unlike manned aircrafts, drones are widely accessible to both law enforcement and private individuals. Additionally, drones are equipped with high-resolution cameras, infrared sensors, and real-time tracking, with capabilities of hovering silently at lower altitudes, navigating tight spaces, and conducting prolonged surveillance.¹ This significantly alters the balance between privacy and public observation. As drones become an increasingly common tool for surveillance, courts must grapple with whether the existing legal framework adequately protects individuals from intrusive monitoring or whether a new approach is necessary to address modern Fourth Amendment concerns. If law enforcement can conduct low-altitude, persistent aerial surveillance of a person’s home without a warrant, does that erode the fundamental privacy protections that *Katz* sought to preserve? Moreover, *Ciraolo* and *Riley* failed to clarify the parameters of general public use, leaving unanswered the question of what altitude level starts to encroach outside

of the naked-eye view, which is significant when dealing with drone surveillance.

As courts begin grappling with these evolving questions, practitioners must take proactive and strategic steps to safeguard their clients’ Fourth Amendment protections, which sometimes may require a more innovative approach. Drawing from the surveillance methods used in *Ciraolo* and *Riley*, defense counsel should scrutinize the surveillance methodology at play, looking at whether drones or similar surveillance technologies have been employed in a manner that surpasses traditional observations from public airspace and thus violates the Fourth Amendment. Counselors should challenge the public-vantage-point doctrine, arguing that drones, unlike traditional aircraft, are not a routine mode of public travel. Key considerations here include whether the surveillance involved prolonged monitoring or targeted observation, as opposed to incidental observations made from routine public travel.

Additionally, a strong defense can be built by going back to the basics and returning to foundational search and seizure principles. Counselors may raise a property-based Fourth Amendment argument, asserting that drones hovering over private property constitute a trespass under traditional notions of the trespass doctrine.

As technology continues to reshape our understanding of privacy, the debate over Fourth Amendment protections in the sky is far from settled. However, the growing prevalence of drone surveillance underscores the urgency for practitioners to navigate this shifting landscape. The strategies outlined here provide a starting point for striking the necessary balance between the government’s investigative authority and an individual’s constitutional protections.

¹ Overview of Drone Capabilities and Potential Risk, Aightsight, <https://www.aightsight.com/blog/overview-of-drone-capabilities-and-potential-risks> (last visited Apr. 11, 2025).

The ZA Editors thank Seena Bahhur for contributing this helpful information. Seena was a second-year law student at Campbell Law School and an extern in the FPD office during the Spring of 2025.



Navigating Ransomware Cases: Roles, Statutory Charges, and Sentencing Trends

Ransomware attacks are increasing. According to Cyberint’s 2024 Annual Report, there were 5,414 ransomware incidents globally—an 11% rise from 2023. The fourth quarter alone saw 1,827 incidents, making it the most active quarter of the year.¹ This surge has caught the atten-

tion of the FBI and DOJ. The FBI's Internet Crime Complaint Center (IC3) reported a 9% increase in ransomware complaints targeting U.S. critical infrastructure sectors in 2024.² Meanwhile, DOJ indictments rose from five in 2023 to twelve in 2024.³

Given the complexity of these schemes, prosecutors have brought ransomware-related charges under various federal statutes. Corresponding sentences for convicted defendants range widely, depending on their role and level of involvement. This article provides a general primer for defense attorneys representing individuals accused of ransomware-related crimes. It outlines how ransomware schemes work, common roles within ransomware operations, applicable statutes, and sentencing outcomes.

I. How Ransomware Works

Ransomware is malicious software designed to encrypt a victim's files or lock access to a system until a ransom is paid, usually in cryptocurrency.⁴ A typical ransomware operation begins with initial access, often gained through phishing or stolen credentials.⁵ Once inside, attackers deploy the ransomware, encrypting files system-wide. The ransomware uses strong cryptographic algorithms to scramble file contents, making them unreadable without a decryption key.⁶ Some variants also modify system settings or overwrite records, effectively locking users out of the operating system and preventing normal access to their data.⁷

After the attack, victims are instructed to pay a ransom in exchange for a decryption key. Increasingly, attackers also steal sensitive data and threaten to publish it—a tactic known as “double extortion.”⁸ If victims pay, the attackers may provide the key and launder the proceeds through cryptocurrency mixing services to obscure the trail.⁹

II. Roles in Ransomware Schemes

Most modern ransomware operations follow the Ransomware-as-a-Service (RaaS) model, where core developers lease their malware to others who execute the attacks.¹⁰ Within this model, four primary roles emerge: Developers or core operators create the ransomware code and maintain supporting infrastructure, such as leak sites.¹¹ Affiliates (also known as deployers) use the malware to conduct attacks and typically receive most of the ransom proceeds. Affiliates are effectively hackers operating as independent contractors, choosing their own targets and infection methods (such as phishing, exploiting vulnerabilities, or using access purchased from brokers) while relying on the core developers for updates, support, and payment infrastructure.¹² Crypters support operations by designing tools to evade antivirus detection and aid in data harvesting and remote access.¹³ Money launderers convert ransom proceeds into fiat currency, often using mixers or shell companies to hide the money trail.¹⁴

While the RaaS model has emerged as the most common form of ransomware, schemes vary

significantly in complexity depending on the number of co-conspirators and the division of labor. Smaller operations, such as early attacks like **Jigsaw**, have often been conducted by lone actors handling all aspects of the scheme.¹⁵ In contrast, large RaaS groups like **REvil** or **Conti** operate with dozens of specialized participants. Nevertheless, even in these larger schemes, individuals sometimes perform multiple roles.¹⁶ For instance, Yaroslav Vasinskyi, linked to REvil, was charged with both deploying ransomware, including the 2021 Kaseya supply-chain attack, and conspiring to launder the ransom proceeds.¹⁷

III. Federal Statutes Used in Prosecution

Prosecutors rely on a range of statutes depending on the defendant's role in the scheme. The Computer Fraud and Abuse Act (18 U.S.C. § 1030) addresses unauthorized access and damage to protected computers.¹⁸ Wire fraud (18 U.S.C. § 1343) is charged when electronic communications are used in furtherance of a fraud scheme.¹⁹ Money laundering statutes (18 U.S.C. §§ 1956-1957) target those handling illicit proceeds.²⁰ Conspiracy (18 U.S.C. § 371) is frequently charged when participants act in concert.²¹ Prosecutors also charge 18 U.S.C. § 875 (d) for extortionate threats and 18 U.S.C. § 982 to authorize asset forfeiture.²²

IV. Sentencing

Sentences vary widely, often based on the defendant's role. Affiliates deeply involved in deployment or coordination generally receive the harshest penalties. Yaroslav Vasinskyi, for example, pled guilty to an 11-count indictment including conspiracy, computer fraud, and money laundering.²³ He participated in deploying over 2,500 ransomware attacks, including deploying the malware, and was sentenced to 13 years and 7 months in prison.²⁴ Daniel Hulea deployed NetWalker ransomware to obtain approximately 1,595 bitcoin in ransom payments, valued at over \$21.5 million. He received a 20-year sentence.²⁵

Others with narrower roles received lighter sentences. Vladimir Dunaev developed browser modifications and malicious tools that aided in credential harvesting and datamining from infected computers, facilitated and enhanced the remote access used by Trickbot ransomware actors, and created program code to prevent the Trickbot malware from being detected by legitimate security software.²⁶ During Dunaev's participation in the scheme, 10 victims in the Northern District of Ohio were defrauded of more than \$3.4 million via ransomware deployed by Trickbot.²⁷ He was sentenced to five years and four months in prison.²⁸ Similarly, his co-conspirator, who was a Trickbot malware developer, rather than a deployer, pleaded guilty to conspiracy to commit computer fraud and was sentenced to two years and eight months in prison.²⁹

V. Conclusion

Modern ransomware prosecutions present unique challenges for defense attorneys. These cases often involve complex, international operations with multiple actors. The broad use of conspiracy and money laundering statutes can result in disproportionate punishment. Effective defense strategies require a detailed understanding of the client's specific role, a close analysis of the government's evidence, and a strong argument for proportionate sentencing.

¹ Adi Bleih, *Ransomware Annual Report 2024*, Cyberint (Jan. 13, 2025), <https://cyberint.com/blog/research/ransomware-annual-report-2024/> (last visited Aug. 1, 2025).

² FBI Internet Crime Complaint Ctr., *2024 Internet Crime Report 6* (Mar. 2025), https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf (last visited Aug. 1, 2025).

³ See Press Releases, U.S. DOJ, <https://www.justice.gov/news/press-releases> (last visited Aug. 1, 2025) (searched "ransomware" and "indict*" or "charged").

⁴ CISA, *Ransomware Guide 2* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Aug. 1, 2025).

⁵ *Id.* at 3-4.

⁶ Bitsight, *What Is Ransomware? Types & Real-Life Examples* (Jan. 2025), [wired.com+1paloaltonetworks.com+1bitsight.com](https://www.wired.com+1paloaltonetworks.com+1bitsight.com) (last visited Aug. 1, 2025).

⁷ CISA, *Petya Ransomware* (July 1, 2017), https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware?utm_ (last visited Aug. 1, 2025).

⁸ CISA, *Ransomware Guide 2* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Aug. 1, 2025).

⁹ *Id.*

¹⁰ Chainalysis, *2024 Crypto Crime Report* 31-33 (2024), <https://go.chainalysis.com/2024-Crypto-Crime-Report.html> (last visited Aug. 1, 2025).

¹¹ Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* 17 (2023), https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf (last visited Aug. 1, 2025).

¹² *Id.* See also Cybersecurity & Infrastructure Sec. Agency, *Understanding Ransomware Threat Actors: LockBit* (June 2023), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a> (last visited Aug. 1, 2025).

¹³ *Id.*

¹⁴ Federal Bureau of Investigation, *Ransomware Abettor Sentenced*, FBI (Dec. 6, 2018), <https://www.fbi.gov/news/stories/ransomware-abettor-sentenced-120618> (last visited Aug. 1, 2025).

¹⁵ Malwarebytes Labs, *Cardiologist Moonlighted as Successful Ransomware Developer* (May 19, 2022), <https://www.malwarebytes.com/blog/news/2022/05/cardiologist-moonlighted-as-successful-ransomware-developer> (last visited Aug. 1, 2025).

¹⁶ Trend Micro, *Unpacking the Structure of Modern Cybercrime Organizations* (Apr. 3, 2023), https://www.trendmicro.com/en_us/research/23/d/unpacking-the-structure-of-modern-cybercrime-organizations-.html#:~:text=Small%20groups%20of%20criminals%20that,service%20in%20the%20cybercrime%20realm (last visited Oct. 15, 2025).

¹⁷ Press Release, U.S. Dep't of Justice, *Ukrainian Arrest-*

ed and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), <https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya> (last visited Aug. 1, 2025).

¹⁸ Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2024).

¹⁹ Wire Fraud Statute, 18 U.S.C. § 1343 (2024).

²⁰ Money Laundering Statutes, 18 U.S.C. §§ 1956-57 (2024).

²¹ Conspiracy Statute, 18 U.S.C. § 371 (2024).

²² Extortion and Asset Forfeiture Statutes, 18 U.S.C. §§ 875(d), 982 (2024).

²³ Press Release, U.S. Dep't of Just., *Sodinokibi/REvil Affiliate Sentenced for Role in \$700 M Ransomware Scheme* (May 1, 2024), <https://www.justice.gov/archives/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme> (last visited Aug. 1, 2025).

²⁴ *Id.*

²⁵ Press Release, U.S. Dep't of Just., *Romanian National Sentenced to 20 Years in Prison in Connection With NetWalker Ransomware Attacks* (Dec. 19, 2024), <https://www.justice.gov/archives/opa/pr/romanian-national-sentenced-20-years-prison-connection-netwalker-ransomware-attacks> (last visited Aug. 1, 2025).

²⁶ Press Release, U.S. Dep't of Just., *Russian National Pleads Guilty in Trickbot Ransomware Scheme* (Nov. 2023), <https://www.justice.gov/archives/opa/pr/russian-national-sentenced-involvement-development-and-deployment-trickbot-malware> (last visited Aug. 1, 2025).

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

The ZA Editors thank Zach Griffith for contributing this helpful information. Zach was a third-year law student at UNC School of Law and was an intern in the FPD office during the Summer of 2025.



Textualism as a Tool in Federal Criminal Defense

It is no secret the Supreme Court of the United States now employs textualism as its primary statutory interpretation methodology.¹ Though its merits are the subject of feverish debate among academics,² the Court's firm textualist bend has reshaped federal criminal defense attorneys' toolboxes. In a series of recent cases, the Court considerably narrowed the reach of several criminal statutes. And this term, the Court will decide *Kousisis v. United States*, 82 F.4th 230 (3d Cir. 2023), *cert. granted*, 144 S. Ct. 2655 (2024), determining how far federal prosecutors may stretch the federal wire fraud statute.

Two recent cases illustrate how textualist readings of criminal statutes scaled back the scope of liability. In *Dubin v. United States*, 599 U.S. 110 (2023), the Court evaluated the terms "uses" and "in relation to" in 18 U.S.C. § 1028A, which mandates a two-year minimum sentence for aggravated identity theft committed during the

scope of a predicate felony. *Id.* at 117. In that case, a doctor misrepresented the qualification of an employee, who performed psychological testing, when submitting Medicaid reimbursements for that testing. *Id.* at 114. The Government charged the doctor with healthcare fraud under 18 U.S.C. § 1347. *Id.* But the Government also contended that this constituted aggravated identity theft under 18 U.S.C. § 1028A(a)(1), which imposes liability when a defendant “during and in relation to any [predicate offense], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person.” *Id.* at 115. In its unanimous decision, the Court labeled the government’s broad reading, where § 1028A(a)(1)’s elements were “automatically satisfied” by the predicate felony, as “staggering.” *Id.* at 115. In reversing the Fifth Circuit, the Court’s decision considerably narrowed when prosecutions can be brought under § 1028A by reading the statute through a textualist lens.

The next year, textualism again worked as a sword cutting into hawkish prosecutions. *Snyder v. United States*, 603 U.S. 1 (2024) limited the application of 18 U.S.C. § 666, which criminalizes theft or bribery in connection with receipt of federal funds. In *Snyder*, the Government charged a mayor with receiving a bribe in violation of § 666. *Id.* at 9-10. The mayor accepted a \$13,000 check from a trucking contractor after the contractor completed work for the city. *Id.* at 9. As defined by § 666, bribery occurs when someone “corruptly solicits or demands . . . accepts or agrees to accept, anything of value from any person, intending to be influenced or rewarded in connection with any business, transaction, or series of transactions.” Bribes are payments or gifts given *before* an official act. *Id.* at 5. Bribes differ from gratuities, which are payments *after* an act is complete. *Id.* The Court narrowly interpreted this statute, concluding that the text of § 666 only bars bribes, not gratuities. *Id.* at 12. The payment received by the mayor was a gratuity and, therefore, fell outside the scope of the statute. Just as in *Dubin*, the Court applied a granular textualist analysis to constrain the reach of prosecutions under the statute.

Statutes rarely exist in a vacuum. Some federal criminal statutes use identical wording. For instance, in *Dubin*, the Court looked to interpretation of the terms “uses” and “during and in relation to” to 18 U.S.C. § 924(c) and compared § 1028A with 18 U.S.C. § 1028’s texts. *Dubin* 559 U.S. at 119 n.4, 121. Cases adopting narrow textualist readings of one criminal statute may persuade lower courts to adopt a more restrictive view of the conduct covered by another statute. When the government seems to stretch the conduct covered by a statute, defense attorneys should look closely at the text. If the prosecution argues that another offense automatically applies as well, defense attorneys can examine *Dubin* and compare its reasoning to the statute at bar. If the charge is for conduct that does not perfectly track to the statute, such as a temporal connection, *Snyder* may prove persuasive.

Though implementing textualist appeals may prove difficult at the trial level, appellate lawyers

may have more space to do so. The appellate forum provides more opportunity to make arguments grounded in detailed statutory interpretation, but trial lawyers must preserve arguments for appeal. Thus, the criminal defense bar at large must know how to employ textualism to argue that a statute does not reach a defendant’s conduct.

Dubin and *Snyder* are not aberrations. They represent a broader trend of textualism narrowing criminal statutes once used broadly. Despite its controversies, in the criminal context, textualism provides a tool defense attorneys can leverage to prevent prosecutors from bringing certain charges. The Court may choose to continue its textualist streak in *Kousisis* this term. As the Court continues to emphasize the text above broader structural considerations, criminal defense attorneys have ample opportunities to advocate for narrow interpretation of criminal statutes.

¹ See William N. Eskridge, Jr. Brian G. Slocum & Kevin Tobia, *Textualism’s Defining Moment*, 123 Colum. L. Rev. 1611, 1616 (2023) (“Textualism is now clearly ascendant and will remain so for the foreseeable future.”).

² See, e.g., James J. Brudney & Lawrence Baum, *Oasis or Mirage: The Supreme Court’s Thirst for Dictionaries in the Rehnquist and Roberts Eras*, 55 Wm. & Mary L. Rev. 483, 492-93 (2013); Anita S. Krishnakumar, *Textualism in Practice*, 74 Duke L.J. 573 (2024).

The ZA Editors thank Brandon Bishop for contributing this helpful information. Brandon was a third-year law student at Duke University School of Law and an extern in the FPD office during the Spring of 2025.



The End of Expert Echoes

The Sixth Amendment’s Confrontation Clause, described by the U.S. Supreme Court as “[o]ne of the fundamental guaranties of life and liberty,”¹ has long safeguarded the accused’s right to confront the witness against them. It is not merely a procedural formality, but a “fundamental right essential to a fair trial”² that the Court must zealously protect from erosion. However, in recent decades, this right has faced mounting pressure from evolving forensic practices, particularly the increasing reliance on what this Article refers to as forensic echoes: expert testimony that transmits the substance of an absent analyst’s conclusions under the guise of independent opinion. These indirect restatements risk circumventing cross-examination and threaten the legal system’s integrity. Therefore, federal criminal practitioners should take note of a key development in Confrontation Clause jurisprudence. In *Smith v. Arizona*, 602 U.S. 779 (2024), the Su-

preme Court held that when a government expert conveys an absent analyst's findings to support their own opinion, those statements are admitted for their truth and thus constitute testimonial hearsay. This ruling intensified the longstanding tension between a defendant's Sixth Amendment right to confrontation and the admissibility of expert testimony under Federal Rules of Evidence 702 and 703.

In *Smith*, a forensic expert testified at trial about a non-testifying analyst's drug analysis. 602 U.S. at 1796. The testifying expert relied on the absent analyst's notes and reports to form an "independent opinion," but in effect, relayed the original conclusions. *Id.* The Court rejected the prosecution's argument that such statements were introduced merely to demonstrate the basis for the testifying expert's opinion. *Id.* at 1791. Instead, it held that the expert's testimony restated "an absent lab analyst's factual assertions to support his own opinion testimony," and that those assertions could "provide that support only if true." *Id.* Because the jury had to accept the original analyst's statements as true to credit the expert's conclusion, this implicated the Confrontation Clause. *Id.* Accordingly, absent the Government demonstrating the original analyst was unavailable and that the defendant had a prior opportunity to cross-examine, such evidence triggers the protections of *Crawford*³ and cannot be admitted, even through the conduit of another expert. *Id.* at 1802. The Court clarified that evidentiary rules, such as Rule 703, which allows experts to rely on out-of-court opinions, do not override constitutional protections. *Id.* at 1808-09.

In the wake of *Smith*, the Fourth Circuit applied its reasoning in *United States v. Seward*, 135 F.4th 161 (4th Cir. 2025), abrogating its surrogate expert precedent and offering a practical pathway for defense challenges to lab-based testimony. In *Seward*, the Fourth Circuit became one of the first federal courts to apply *Smith*, confronting nearly identical facts. 135 F.4th at 164. Trevor Seward was convicted of murdering a federal mail carrier. *Id.* At trial, the Government introduced testimony from a DNA expert who admitted that she was not "hands-on with the evidence samples." *Id.* at 168. Instead, she reviewed the notes of a non-testifying analyst who did test the samples and formed an opinion based on that work. *Id.* On appeal, the Fourth Circuit concluded this testimony likely violated the Confrontation Clause under *Smith*. *Id.* at 169. Although the expert avoided directly quoting the absent analyst's conclusions, the Court found that her testimony nonetheless rested on those conclusions and was admitted to show the basis of her expert opinions. *Id.* As in *Smith*, the testifying expert's opinion was meaningful only if the original analyst's statements were true. *Id.*

The Fourth Circuit explicitly abrogated its earlier decision in *United States v. Summers*, 666 F.3d 192 (4th Cir. 2011), which had permitted surrogate expert testimony so long as the witness claimed to form independent opinions. *Id.* at 169. The Court found that approach "no longer tenable" in light of *Smith*'s holding that "surrogate testimony" does not cure a Confrontation Clause violation.

Id. The Court reaffirmed that "the ability to cross-examine someone else is insufficient" and that defendants have "a right to cross-examine the testing analyst about what she did and how she did it and whether her results should be trusted." *Id.*

While the Court ultimately deemed the Confrontation Clause error harmless in *Seward*, federal defenders should not overlook the decision's broader value. *Id.* at 169-70. *Smith* and *Seward* offer a blueprint for challenging forensic evidence when the Government relies on a substitute expert, or a testifying expert relies on the lab work of an absent analyst. At the pretrial stage, defense counsel should consider moving to exclude any expert testimony derived from lab reports or notes authored by someone other than the testifying witness. Counsel should urge courts to require the Government to produce the original analyst for cross-examination, particularly where the testimonial nature of the statements is clear. Voir dire on the expert's firsthand involvement—or lack thereof—can set the stage for a robust Confrontation Clause challenge. Finally, during trial, cross-examination should emphasize the testifying expert's reliance on absent declarants and frame their testimony as hearsay offered for its truth.

Together, *Smith* and *Seward* mark a pivotal shift in the constitutional limits on surrogate expert testimony. They reinvigorate confrontation rights in forensic-heavy prosecutions and reassert the Sixth Amendment's demand for live, testable witnesses, not secondhand summaries. Forensic science cannot operate on blind trust. Where the expert's opinion cannot stand without crediting the absent analyst's work, the Confrontation Clause applies. The Supreme Court has now made clear: forensic echoes are inadequate. If prosecutors want to rely on lab results, they must bring the original analyst to court.

¹ *Kirby v. United States*, 174 U.S. 47, 55-56 (1899).

² *Pointer v. Texas*, 380 U.S. 400, 403 (1965).

³ *Crawford v. Washington*, 541 U.S. 36, 50 (2004).

The ZA Editors thank Elizabeth Candelmo for contributing this helpful information. Elizabeth was a third-year law student at the University of Pittsburgh School of Law and was an intern at the FPD office during the Summer of 2025.



Expert Testimony on Classwide Mental States After *Diaz v. United States*

Rule 704(b) of the Federal Rules of Evidence provides that "[i]n a criminal case, an expert witness must not state an opinion about whether the defendant did or did not have a mental state or condition that constitutes an element of the crime charged or of a defense."¹ This rule preserves these ultimate determinations for the

jury.² Interpreting Rule 704(b), however, the United States Supreme Court held in *Diaz v. United States* that an expert may state an opinion about whether a class of people that includes the defendant generally does or does not have a mental state that constitutes an element of the crime.³ For example, in that case, the defendant was charged with “knowingly” importing methamphetamine into the United States from Mexico.⁴ To refute this necessary mental state, the defendant argued that she did not know there were drugs in the car that she drove across the border.⁵ But, to rebut this at trial, the government’s expert witness testified that “in most circumstances, the driver [a class that includes the defendant] knows they are hired . . . to take the drugs from point A to point B” because drug-trafficking organizations want to avoid the risks of using unknowing couriers.⁶

The Court held that this type of expert testimony did not violate Rule 704(b).⁷ It reasoned that Rule 704(b) applies only to opinions about “whether [the defendant] herself knowingly transported methamphetamine,”⁸ differentiating between opinions about “most couriers” and those about “all couriers,” as the latter necessarily includes an opinion about the defendant herself.⁹ And because the government’s expert did not testify to that narrow claim, but, rather, only to “the knowledge of most drug couriers,” his testimony did not violate Rule 704(b).¹⁰ In concurrence, Justice Jackson reaffirmed that defense counsel may use the Court’s interpretation of Rule 704(b) to support their own admission of expert testimony negating a criminal mental state and/or supporting a defense mental state.¹¹ Additionally, in dissent, Justice Gorsuch raised other rules of evidence that defense counsel may use to undermine the admissibility of the type of expert testimony permitted in this case.¹² This article explores these alternative avenues for how defense counsel may use *Diaz* to support this kind of defense expert testimony or limit the admissibility of similar government expert testimony.

I. Using Rule 704(b) and *Diaz* for Defense Experts

Just as the government in *Diaz* used expert testimony on the criminal mental state of a class that includes the defendant to prove the presence of that mental state, defense counsel can also use classwide expert testimony to negate that criminal mental state or support the mental state of a defense. Specifically, defense counsel may use expert testimony to argue that this particular defendant is not like “most” of the class or that he better fits within a different class of which “most” people do not have the required criminal mental state.¹³ For example, if relevant, counsel may use expert testimony that most people with the defendant’s level of Autism are unable to form the required criminal intent.¹⁴

Additionally, in arguing self-defense, counsel may use expert testimony that most people in a given situation would find the use of force reasonably necessary or the threat of harm sufficiently imminent.¹⁵ Experts can explain, for example, how battered woman syndrome affects a person’s mental

state as it relates to the elements of a perfect or imperfect self-defense.¹⁶ Similarly, in arguing insanity,¹⁷ counsel may use expert testimony that most people with the defendant’s severe mental disease or defect are unable to appreciate the nature and quality of the wrongfulness of their acts in the situation constituting the offense.¹⁸

II. Using Rule 702 and *Daubert* Against Government Experts

Rule 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc.* allow an expert to “help the trier of fact to understand the evidence or to determine a fact in issue” only if he is qualified by “knowledge, skill, experience, training, or education.”¹⁹ The expert’s opinion must further be “based on sufficient facts or data” and be the “product of reliable principles and methods.”²⁰ Defense counsel may use Rule 702 and *Daubert* to attack a government expert’s qualifications, such as whether their methodology (i.e. their general experience) can provide a sufficient basis²¹ and can be reliably applied²² to support an opinion about the specific issue of mental states. Using *Diaz* as an example, counsel may question whether the expert’s experience relates only to general drug-trafficking-organization practices or whether he has specific experience regarding the organizations’ drug-courier practices and, further, drug couriers’ mental states. If the latter, how extensive was this more specific experience? Did he have experience with many different organizations’ drug-courier practices or just a select few? Is his experience based solely on couriers who were arrested and convicted, or does he also have experience with those who did not know about the drugs? The overall inquiry examines the extent to which the expert’s sample of experiences is skewed and self-validating and whether his general experiences can provide a sufficient and reliable basis for the specific opinion at issue regarding mental states.

Further, defense counsel can point to the lack of any corroborating studies or other forms of validation supporting the expert’s methods²³ and whether the expert’s analysis considered alternative explanations.²⁴ Additionally, counsel should be cognizant of when an expert disregards his role of helping the fact-finder understand confusing evidence, and instead, simply opines on whether the defendant’s explanation of events is a credible one. Assessing credibly lies solely with the fact-finder and supplanting that role is impermissible.²⁵ Finally, even if these attacks cannot prevent the expert from testifying, counsel can use them to discredit their testimony during cross-examination. Counsel can also rely on these weaknesses to argue their particular defendant is not like “most” of the class as narrowly defined by the expert’s skewed experience.

III. Using Rules 401, 402, and 403 Against Government Experts

Rules 401 and 402 allow the admission of evidence only if it is relevant.²⁶ However, defense counsel can argue that “[a] government] expert

opinion about the mental state of ‘most’ people like the defendant is not ‘about’ the defendant’s mental state, [so] it is hard to see how that opinion might be relevant.”²⁷ Its lack of relevance is magnified where counsel can point to specific reasons why this defendant is not like “most,” and therefore not like anyone the expert is opining about. Further, Rule 403 allows a court to “exclude [even] relevant evidence if its probative value is substantially outweighed by a danger of . . . unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.”²⁸ On balance, expert testimony on class-wide mental states substantially risks misleading the jury and unfairly prejudicing the defendant by impermissibly encouraging the jury to substitute the class’s mental state for that of the defendant’s. This risk is exacerbated by the excessive weight jurors assign to the government and how the government’s imprimatur further carries onto their expert.²⁹ Finally, even if these attacks cannot prevent the expert from testifying, counsel can use them to argue for jury instructions that limit the scope of the jury’s consideration of the expert’s opinion.

¹ Fed. R. Evid. 704(b).

² *Id.* (“Those matters are for the trier of fact alone.”); *Diaz v. United States*, 602 U.S. 526, 532 (2024).

³ *Diaz*, 602 U.S. at 528.

⁴ *Id.* at 529.

⁵ *Id.*

⁶ *Id.* at 530-31.

⁷ *Id.* at 534.

⁸ *Id.*

⁹ *Id.* at 535-36 (emphasis in original).

¹⁰ *Id.* at 534 (emphasis in original).

¹¹ *Id.* at 540-41 (Jackson, J., concurring).

¹² *Id.* at 553-55 (Gorsuch, J., dissenting) (discussing Federal Rules of Evidence 402, 403, and 702).

¹³ See, e.g., *Diaz*, 602 U.S. at 539 (Jackson, J., concurring) (“Notably, however, the Government was not the only party that relied on this type of mental-state evidence during the trial. Diaz called an automobile specialist who testified that a driver of her particular car would almost certainly not know that it contained drugs.” (emphasis in original)).

¹⁴ For a discussion of this argument, see Monique Chiacchia, *Autism Spectrum Disorder and the Criminal Justice System*, Purdue Glob. (April 5, 2016), <https://www.purdueglobal.edu/blog/criminal-justice/autism-and-the-criminal-justice-system/#:~:text=Although%20most%20with%20an%20ASD,King%20&%20Murphy%2C%202014>.

¹⁵ See *Bianchi v. Brown*, 111 F.4th 438, 449 (4th Cir. 2024) (describing that self-defense requires that use of force be reasonably necessary against an impending threat).

¹⁶ Jessica R. Holliday, Dale E. McNiel, Nathaniel P. Morris, David L. Faigman & Renee L. Binder, *The Use of Battered Woman Syndrome in U.S. Criminal Courts*, J. Am. Acad. Psychiatry & L., 2022, at 1, 3-4 (discussing the use of expert testimony on battered woman syndrome to prove (im)perfect self-defense). See generally Bailey Pierce, Note, *Requiem for a Survivor: The Use of Battered Woman Syndrome in Acquitting Survivors of Abuse*, Ky. L.J., Apr. 2024, at 1 (surveying the use and admissibility of battered woman syndrome in duress defense cases); Dylan Uhrig, Note, *Why Didn't You Leave?: Resolving the Circuit Split on Admitting Battered Woman Syndrome Testimony for Duress Defenses*, 34 U. Fla. J. L. & Pub. Pol’y 431 (2024) (arguing that the federal circuit split on battered woman syndrome be resolved in favor of admissibility).

¹⁷ See 18 U.S.C. § 17 (The insanity defense requires that “at the time of the commission of the acts constituting the offense, the defendant, as a result of a severe mental disease or defect, was unable to appreciate the nature and quality or the wrongfulness of his acts.”); see also 637. *Insanity—Present Statutory Test—18 U.S.C. § 17(a)*, U.S. Dep’t Just., <https://www.justice.gov/archives/jm/criminal-resource-manual-637-insanity-present-statutory-test-18-usc-17a> (last visited Mar. 7, 2025) (explaining the insanity defense test under the Insanity Defense Reform Act).

¹⁸ See Jeffrey S. Janofsky, Anne Hanson, Philip J. Canilis, Wade C. Myers & Howard Zonana, *AAPL Practice Guideline for Forensic Psychiatric Evaluation of Defendants Raising the Insanity Defense*, J. Am. Acad. Psychiatry & L., 2014, at S3, S6-S8 (explaining the test); *id.* at S28-S33 (guiding experts on how to frame their reports for insanity defenses).

¹⁹ Fed. R. Evid. 702(a); see *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 593-94 (1993) (listing potential factors for evaluating experts); *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 141 (1999) (extending *Daubert*’s holding to non-scientific experts).

²⁰ Fed. R. Evid. 702(b)-(c); see *Daubert*, 509 U.S. at 593-94.

²¹ See e.g., *United States v. Garcia*, 752 F.3d 382, 391 (4th Cir. 2014) (admitting expert testimony of drug trafficker’s coded language based on, among other things, the expert’s experience “monitor[ing] dozens of wiretaps, listening to thousands of intercepted phone calls in the process,” and “training which specifically included exposure to drug traffickers’ use of coded language”).

²² See Fed. R. Evid. 702 advisory committee’s note to 2000 amendment (“If the witness is relying solely or primarily on experience, then the witness must explain how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts.”).

²³ See *id.* (“While the relevant factors for determining reliability will vary from expertise to expertise, the amendment rejects the premise that an expert’s testimony should be treated more permissively simply because it is outside the realm of science. An opinion from an expert who is not a scientist should receive the same degree of scrutiny for reliability as an opinion from an expert who purports to be a scientist.”).

²⁴ See, e.g., *United States v. Chikvashvili*, 859 F.3d 285, 294 (4th Cir. 2017) (noting that expert testimony may be inadmissible where the expert “fails to take serious account of other potential causes . . . [such] that it cannot provide a reliable basis” or “can offer ‘no explanation for why she has concluded [that an alternative cause] was not the sole cause.’” (alteration and emphasis in original) (quoting *Westberry v. Gislaved Gummi AB*, 178 F.3d 257, 265 (4th Cir. 1999)).

²⁵ See *Jones v. Solomon*, 90 F.4th 198, 209 (4th Cir. 2024) (“[W]hen laypersons are just as capable of comprehending the primary facts and of drawing correct conclusions from them as are experts, expert testimony may properly be excluded.” (citation and quotation marks omitted)); *United States v. Fuertes*, 805 F.3d 485, 495 (4th Cir. 2015) (“[T]he district court must exclude expert testimony on issues of witness credibility.”).

²⁶ Fed. R. Evid. 402; see Fed. R. Evid. 401 (“Evidence is relevant if (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.”).

²⁷ *Diaz*, 602 U.S. at 553 (Gorsuch, J., dissenting).

²⁸ Fed. R. Evid. 403.

²⁹ See *United States v. Young*, 470 U.S. 1, 18-19 (1985)

(discussing how the “imprimatur of the Government [] may induce the jury to trust the Government’s judgment rather than its own view of the evidence”).

The ZA Editors thank Lexie Siegel for contributing this helpful information. Lexie was a third-year law student at UNC School of Law and an extern in the FPD office during the Spring of 2025.



Chapter One Guidelines: Your Sentencing Lifeline

On January 5th, 2024, Mr. Rodriques Evans gained an opportunity to reduce his eighty-year prison sentence for conspiring to transport and sell Schedule one drugs. See *United States v. Evans*, 90 F.4th 257, 260-61 (4th Cir. 2024). On appeal, the Fourth Circuit Court of Appeals remanded his case, allowing him to challenge the total drug weight attributed to him in the conspiracy. See *id.* The source of Mr. Evans’ good fortune was no mere windfall, but the result of his attorney’s diligent examination of Chapter One of the United States Sentencing Guidelines (U.S.S.G.). Mr. Evans’ attorney successfully argued that the District Court’s reliance on the *Pinkerton Doctrine* to assign liability failed to follow the Guideline’s instructions of reviewing conspiracy liability. See *id.* at 261-63. As a result, the Court of Appeals remanded the case, enabling Mr. Evans to challenge the total drug weight attributed to him in the conspiracy and argue for a sentence reduction. See *id.* at 264-65.

Mr. Evans’ case is not unique — it is a part of a broader trend of opinions reminding District Courts not to rely on *Pinkerton* liability for sentencing purposes. Liability under the sentencing guidelines can result in a reduced sentence compared to what might be imposed under *Pinkerton*. In general, *Pinkerton* liability holds defendants accountable for all foreseeable acts of co-conspirators that further the conspiracy’s objectives. See *Pinkerton v. United States*, 328 U.S. 640, 648 (1946). As a result, a defendant’s sentence can increase dramatically if the court determines drugs seized by another conspirator are part of the overall scheme, attributing the total weight of those drugs to the defendant. However, liability under the U.S.S.G. is more conservative than *Pinkerton*’s broad approach. Thus, to ensure proper sentencing and avoid overly harsh penalties, practitioners should be mindful of the specific requirements set forth in the guidelines. This article will explore these requirements in further detail.

Proper sentencing under the U.S.S.G. requires the court to establish liability using the methods outlined in Chapter One, Section 1B1.3. See *United States v. Gilliam*, 987 F.2d 1009, 1012-13 (4th Cir. 1993). Under §1B1.3, the court must first determine the scope of the criminal activity the defendant agreed to jointly undertake, using particularized facts. See *United States v. Flores-*

Alvarado, 779 F.3d 250, 256 (2015). The court must then make specific findings about the defendant’s acts and whether they were within the conspiracy’s scope. See *id.* at 255. Finally, the court must make particularized findings to determine if the defendant could foresee the conduct of other co-conspirators based on its previous conclusions. See *id.* at 256. As a result, liability in a multi-defendant drug conspiracy may differ from *Pinkerton* liability, since each defendant could be held accountable for different quantities of drugs, depending on the specific evidence presented. See *Gilliam*, 987 F.2d at 1013.

Analysis under §1B1.3 applies to all aspects of reviewing the defendant’s conduct, including when determining applicable enhancements. See *United States v. Bright*, 125 F.4th 97, 102 (4th Cir. 2025). For example, in *Bright*, the Court of Appeals overturned the District Court’s finding that the defendant was a manager of a drug-dealing enterprise, citing that the District Court did not support its conclusion with specific, detailed findings. See *id.* at 103-04. The District Court applied a three-point enhancement, concluding that Mr. Bright was a manager in a five-person drug-dealing conspiracy. *Id.* at 99-100. However, the District Court erred by attributing Mr. Bright’s managerial-like role to the remaining four defendants indicted when the facts only supported a finding that Mr. Bright acted as a manager to one defendant. *Id.* On review, the Court of Appeals ruled that §1B1.3 required the District Court to make particularized findings showing that Mr. Bright was acting as a manager for each of the four other defendants. *Id.* at 103.

A court can make particularized findings by relying on the defendant’s pre-sentence report (PSR), if offered by the prosecution. Since the law presumes PSRs to be factually correct, defense counsel must object to inaccurate or unreliable findings within them. See *Gilliam*, 987 F.2d at 1014. The defendant does not need to object to all facts in the PSR, rather, it is sufficient to show that the facts the government uses to support its inferences lack a “sufficient indicia of reliability to support” the asserted conclusions. See *id.* For example, in *United States v. Gilliam*, the Court of Appeals found that the District Court’s reliance on ambiguous information in the PSR to estimate the quantity of drugs attributable to Mr. Gilliam was an abuse of discretion. *Id.* Therefore, the court vacated the sentence and remanded the case. See *id.* at 1015.

When preparing for sentencing, the cases of *Evans*, *Bright*, *Gilliam*, and their cohort underscore the critical importance of thoroughly reviewing the PSR and closely examining Chapter One of the sentencing guidelines. By understanding the detailed requirements of Chapter One, such as the proper application of conspiracy liability and the need for particularized findings, defense attorneys can ensure that the court grounds its decisions in an accurate assessment of their client’s conduct. A comprehensive review of these guidelines enables the identification of potential procedural errors, ensuring that defense attorneys

can challenge any reliance on flawed conclusions—such as improper applications of *Pinkerton* liability and use of ambiguous drug quantity information. Ultimately, a deep familiarity with Chapter One will secure the client’s best interests and safeguard against unjust outcomes.

The ZA Editors thank Josh DuBois for contributing this helpful information. Josh was a second-year law student at UNC School of Law and was an extern in the FPD office during the Spring of 2025.



Targeted or Typical? Fighting the Vulnerable Victim Label

Sentencing is a critical period for a person convicted of a federal crime. Defense counsel must work to mitigate the sentence to achieve the fairest possible outcome. During sentencing, it is essential to prevent the addition of enhancements where possible, such as rebutting claims of vulnerable victims. In *United States v. Lawson*, the Fourth Circuit reminded us how to make a strong argument against the vulnerable victim enhancement at sentencing.¹ The United States Sentencing Guidelines Manual § 3A1.1(b)(1) states that a person’s offense level may be increased “[i]f the defendant knew or should have known that a victim of the offense was a vulnerable victim,” and increased further if “the offense involved a large number of vulnerable victims.” This enhancement requires a finding of two “fact-based” prongs: (1) an explanation as to “why advanced age or some other characteristic made one or more victims unusually vulnerable to the offense conduct,” and (2) “why the defendant knew or should have known of this unusual vulnerability.”²

The first step is to address the vulnerability prong—that is, to attack the causal link between age or another characteristic and increased susceptibility to a specific offense. The defendant may emphasize that not all crimes committed against a particular group should trigger the vulnerable victim enhancement.³ A crime committed against the elderly, for example, does not necessarily always mean that vulnerability was present.⁴ Therefore, the Government is responsible for showing a link between the crime the defendant was convicted of and why the victim was “particularly susceptible” to that criminal conduct.⁵ Defense counsel should argue that their client’s age, physical or mental condition, or status did not play a meaningful role in the commencement of the offense or in rendering the victim unusually susceptible compared to the general population.⁶ When appropriate, counsel may also highlight the absence of cognitive impairment or other specific vulnerabilities that would connect the characteristic to increased risk of susceptibility.⁷

Furthermore, it is important to emphasize that vulnerability should be assessed in relation to the typical victim of the particular offense.⁸ Indeed, it is no longer necessary for the Government to

prove that the accused person targeted a victim or victims specifically because of their vulnerability.⁹ However, *Lawson* describes the intentional targeting of the elderly in telemarketing schemes and explains that district courts are “entitled to infer that [elderly] victims were targeted due to their age-related vulnerability.”¹⁰ Therefore, defense counsel must be prepared to distinguish their case from this paradigm by showing that the defendant’s conduct did not rely on or exploit the alleged vulnerability.¹¹ Where the victims displayed no unusual characteristics or where the accused person had no role in identifying or contacting victims, counsel should argue that the enhancement lacks the necessary factual basis and should not apply.¹²

In attacking the second prong, there should be a challenge to the accused person’s knowledge of the victim’s vulnerability.¹³ One method is to dispute pattern-based assumptions.¹⁴ In *Lawson*, the PSR relied on assumptions about “Jamaican Lottery Scam[s]” and not just case-specific evidence.¹⁵ However, arguments may still be made to refute these points.¹⁶ The vulnerable victim enhancement should not rest on generalized assumptions about victim populations, and sentencing courts must draw a specific, supported connection between the accused person’s conduct and awareness of the victim’s heightened susceptibility.¹⁷ When the PSR or Government relies on stereotypes about a fraud scheme’s typical victims, defense attorneys should argue against judicial notice of general patterns in specific cases.

Preparing to argue against inappropriate enhancements for victim characteristics can meaningfully affect your client’s sentence. Though the application of the vulnerable victim enhancement may appear inevitable in some cases, the two-prong requirement permits well-grounded arguments. Defense counsel should scrutinize the vulnerability of the victim and the accused person’s actual knowledge of the victim’s susceptibility to the crime. By challenging overgeneralizations, creating a fact-specific record, and forcing the Government to meet its burden with deliberateness, clients may be in a position to obtain a more favorable sentencing outcome.

¹ See *United States v. Lawson*, 128 F.4th 243, 248-52 (4th Cir. 2025).

² *United States v. Shephard*, 892 F.3d 660, 670 (4th Cir. 2018) (quoting *United States v. Llamas*, 599 F.3d 381, 388 (4th Cir. 2010)).

³ See *Lawson*, 128 F.4th at 250 (“[C]ourts should not apply a blanket assumption that an advanced age is sufficient to render a victim vulnerable and thus that not every crime committed against an older person should automatically be enhanced.”) (internal quotation marks and citation omitted).

⁴ *Lawson*, 128 F.4th at 250.

⁵ See *Lawson*, 128 F.4th at 250 (quoting U.S.S.G. § 3A.1 cmt. n. 2).

⁶ *Id.* at 251.

⁷ *Id.*

⁸ See *id.* at 250 (contextualizing the increased susceptibility of elderly victims in telemarketing schemes).

⁹ *United States v. Luong*, 125 F.4th 147, 159 n.3 (4th

Cir. 2025) (stating that since Amendment 521 was adopted by the Sentencing Commission in 1995, the “targeting” requirement is no longer necessary for the vulnerable victim enhancement).

¹⁰ *Lawson*, 128 F.4th at 251.

¹¹ See *id.* (noting the “common sense” link between the crime and the victims’ vulnerability).

¹² See *id.*

¹³ *Id.* at 250.

¹⁴ *Id.* at 251 (discussing the stereotypical “Jamaican lottery scam”).

¹⁵ *Id.*

¹⁶ *United States v. McCall*, 174 F.3d 47, 50 (2d Cir. 1998).

¹⁷ See *id.*

The ZA Editors thank Aleah Wordsworth for contributing this helpful information. Aleah was a third-year law student at UNC School of Law and an intern in the FPD office during the Summer of 2025.



The Status of Status Points: The Effect of Amendment 821 and Barrett on Federal Sentencing

Every year, the United States Federal Sentencing Commission “reviews and refines the [Federal Sentencing Guidelines (USSG)] in light of congressional action, decisions from courts of appeals, sentencing-related research, and input from the criminal justice community.”¹ In November 2023, the Commission enacted Amendment 821, which, in part, affected the impact of “status points” on a defendant’s sentencing range.² In 2025, the Fourth Circuit interpreted Amendment 821 in a defense-favorable way in *United States v. Barrett*.³

For context, prior to Amendment 821’s enactment, status points ordinarily affected a defendant’s criminal history category.⁴ If the defendant committed the instant offense while they were still serving a sentence for an unrelated case (i.e., while on probation, parole, etc.), the defendant’s number of criminal history points was increased.⁵ At that time, USSG § 4A1.1 added two points to a defendant’s criminal history score in this circumstance.⁶ However, Amendment 821 struck the previous provision and in its place inserted the following: “Add 1 point if the defendant (1) receives 7 or more points under subsections (a) through (d), and (2) committed the instant offense while under any criminal justice sentence, including probation, parole, [etc.].”⁷ In essence, under the current Guidelines, a defendant can receive one status point at the most, rather than two, and a defendant will receive zero status points if they have less than seven criminal history points. Though Amendment 821 may not affect sentencing in every case, it certainly did in Melissa Barrett’s.⁸

Melissa Barrett was serving a 168-month sentence for federal drug offenses when Amendment 821 took effect.⁹ When Ms. Barrett was originally sentenced, her criminal history score was 3: one point for her prior criminal misconduct and two sta-

tus points because she committed the federal offense while on probation.¹⁰ Ms. Barrett’s total offense level was 33, which included a three-level reduction for acceptance of responsibility and no other enhancements (i.e., specific offense characteristics).¹¹ Ms. Barrett’s criminal history category (Category II) and her offense level (33) produced a sentence range of 151 to 188 months’ imprisonment.¹² The sentence imposed, 168 months, was in the middle of the range.¹³

When Amendment 821 took effect, the U.S. Probation Office found Ms. Barrett eligible for a sentence reduction.¹⁴ With Amendment 821’s effect on status points and Ms. Barrett’s original criminal history score of 1, her criminal history score dropped from 3 points to 1 point, putting her in Criminal History Category I instead of Category II.¹⁵ The Probation Office calculated that Ms. Barrett’s new guideline range (with a Criminal History Category I and an unchanged offense level of 33) would be 135–168 months, and noted that a revised sentence of 150 months “would represent a proportionate reduction in [Ms.] Barrett’s sentence.”¹⁶ The Government agreed that Ms. Barrett’s sentence should be reduced to 150 months.¹⁷

Ms. Barrett, however, disagreed with the Government.¹⁸ While Ms. Barrett agreed that Amendment 821 affected her Criminal History Category, she argued that Amendment 821 should affect her offense level: “Because [Ms. Barrett] now had only a single criminal history point under § 4A1.1, she was newly eligible for a two-level offense reduction under § 2D1.1(b)(17).”¹⁹ According to Ms. Barrett’s argument, if her offense level was to be reduced by two levels to 31, and with her amended criminal history score, her new guideline range would be 108–135 months, with a revised sentence of 120 months, rather than 150 months, representing the proportionate reduction.²⁰

The district court sided with the Government, finding that Ms. Barrett was eligible for a reduced sentence of 150 months, rather than 120.²¹ The district court found that Amendment 821 should only modify Ms. Barrett’s criminal history score, not her offense level.²² Ms. Barrett appealed the district court’s decision.²³

The Fourth Circuit vacated the district court’s judgment and remanded the case.²⁴ In doing so, the Court focused on the directive in 18 U.S.C. § 3582(c)(2) that a sentence reduction “must be ‘consistent with applicable policy statements issued by the Sentencing Commission.’”²⁵ This brought the Court to consider “the provision most directly at issue” in the case: USSG § 1B1.10.²⁶ Section 1B1.10 states the following:

In determining whether, and to what extent, a reduction . . . is warranted, the court shall determine the amended guideline range that would have been applicable to the defendant if the [retroactive amendment] had been in effect at the time the defendant was sen-

tenced. In making such determination, the court shall substitute only the [retroactive amendment] for the corresponding guideline provisions that were applied when the defendant was sentenced and shall leave all other guideline application decisions unaffected.²⁷

Because the policy statement indicates that the guideline range must be amended based on the retroactive amendment, and a guideline range is always “the product of both a criminal history category and offense level,” the Court found it was “necessary to account not only for Amendment 821’s impact on [Ms.] Barrett’s criminal history score . . . , but also its direct effect on her eligibility for a lower offense level.”²⁸ The Court pointed out that “this is an unusual case, in that Guidelines closely and directly connect . . . a defendant’s criminal history score under § 4A1.1 to both her criminal history category and her qualification for a two-level offense adjustment under § 2D1.1(b) (17).”²⁹ However, “[w]here an amendment has this kind of direct impact on two provisions integral to a defendant’s ‘amended guideline range,’ retroactive application of that amendment means accounting for both.”³⁰ The Court remanded the case back to the district court to determine whether Ms. Barrett qualified for the offense-level reduction under § 2D1.1(b)(17) based on a proper reading of Amendment 821.³¹

From 2016 to 2021, over a third (37.5%) of federal offenders received two status points.³² For 61.5 % of the offenders that received two status points, including the status points resulted in a higher criminal history category.³³ Based on a plain reading of Amendment 821, for offenders who received status points that resulted in a higher criminal history category, the retroactive application of Amendment 821 could lead to a sentence reduction. Additionally, with the Fourth Circuit’s decision in *United States v. Barrett*, sentences could be even more meaningfully reduced. It will become important for federal practitioners to calculate sentence reductions for their clients whose sentences were affected by status points based on Amendment 821, as well as *Barrett*, when their clients’ offense levels and criminal history categories had some level of interplay.

¹ Policymaking, U.S. SENT’G COMM’N, <https://www.ussc.gov/policymaking#:~:text=Each%20year%2C%20the%20Commission%20reviews,went%20into%20effect%20in%201987> (last visited July 14, 2025).

² See U.S. SENT’G GUIDELINES MANUAL supp. to app. C, amend. 821, part A (U.S. SENT’G COMM’N 2023). See Amendment 821, U.S. SENT’G COMM’N, <https://www.ussc.gov/guidelines/amendment/821> (last visited July 14, 2025), for a readily available online version of the amendment.

³ See 133 F.4th 280 (4th Cir. 2025).

⁴ U.S. SENT’G COMM’N, REVISITING STATUS POINTS 1 (June 2022), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2022/20220628_Status.pdf (last visited July 14, 2025).

⁵ *Id.*

⁶ USSG supp. to app. C, amend. 821, part A.

⁷ *Id.*

⁸ See *Barrett*, 133 F.4th at 288–89.

⁹ *Id.* at 281.

¹⁰ *Id.* at 282.

¹¹ See *id.* at 283.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.* at 283–84.

¹⁷ *Id.* at 284.

¹⁸ *Id.*

¹⁹ *Id.* Note that Ms. Barrett was sentenced under the 2016 version of the Guidelines. *Id.* at 282, n.1. The instant two-level reduction appears as § 2D1.1(b)(18) in the current version of the Guidelines. See *id.* Section 2D1.1(b)(18) of the current Guidelines provides the following: “If the defendant meets the criteria set forth in paragraphs (1)–(5) of subsection (a) of § 5C1.2 (Limitation on Applicability of Statutory Minimum Sentences in Certain Cases), decrease by 2 levels.” The Court describes the § 2D1.1(b)(17) two-level offense reduction in the following way: “The first criterion for this reduction is that the ‘defendant does not have more than 1 criminal history point.’ That was enough to render Barrett, with her three criminal history points, ineligible at the time of her original sentencing. Under the remaining criteria, whether a defendant qualifies turns on whether her offense was violent, her role in the offense, and the extent of her cooperation with the government. If a defendant meets all of the criteria, she automatically receives the two-level reduction.” *Barrett*, 133 F.4th at 282 (citation modified).

²⁰ *Id.* at 284.

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ *Id.* at 289.

²⁵ *Id.* at 283 (quoting 18 U.S.C. § 3582(c)(2)).

²⁶ *Id.*

²⁷ *Id.* (quoting USSG § 1B1.10).

²⁸ *Id.* at 285.

²⁹ *Id.* at 287.

³⁰ *Id.* (citation modified).

³¹ *Id.* at 289.

³² REVISITING STATUS POINTS, *supra* note 4, at 2.

³³ *Id.*

The ZA Editors thank Amy Bernhard for contributing this helpful information. Amy was a third-year law student at Campbell University School of Law and an extern in the FPD office during the Summer of 2025.



LEGAL UPDATES

4th Circuit Update

For up-to-date summaries and commentary on Fourth Circuit cases and federal law, check <http://circuit4.blogspot.com>. For daily, published Fourth Circuit opinions, visit <https://www.ca4.uscourts.gov/opinions>.

U.S. Supreme Court Update

For up-to-date summaries and commentary on Supreme Court criminal cases and federal law, check <http://ussc.blogspot.com>. Be sure to click on “U.S. Supreme Court Case Summaries” under Links and Resources and scroll down to download the PDF summary.

Amended Rules and Guidelines Update

Rules of Criminal Procedure and Evidence¹

There are no amendments to the rules of criminal procedure or evidence for the Eastern District of North Carolina since those that went into effect May 2023. For more information regarding these amendments, please visit the Winter 2024 edition of the *Zealous Advocate*.

There are no amendments to the federal rules of criminal procedure or evidence since those that went into effect December 2023. For more information regarding these amendments, please visit the Winter 2022 edition of the *Zealous Advocate*.

Rules of Appellate Procedure²

Appellate Procedure Rule 39: Costs

The Advisory Committee wishes to change Rule 39 to uphold the decision from *City of San Antonio v. Hotels.com*, 141 S. Ct. 1628 (2021). All changes to Rule 39 will go into effect December 1, 2025. Amendments to Rule 39 seek to accomplish four main goals.

First, the amendment clarifies how the court of appeals is the entity that may decide which parties bear the burden of the costs and what percentages of costs are applicable while the court of appeals or the district court is responsible for calculating and taxing exact costs. Second, Rule 39 now supports the findings in *Hotel.com* where both costs taxed by the court of appeals and the district court are subject to the court of appeals’ allocation of costs. Third, the amendment creates guidelines for motions for reconsidering the costs of appeals, asserting that said motions must not be delayed while acknowledging the right of the court of appeals to make a determination on said motions. Fourth, the new version of Rule 39 lists costs taxable by the court of appeals alongside costs taxable by the district court.

United States Sentencing Guidelines³

Career Offender

The proposed amendment aims to resolve the discrepancies that have occurred in court decisions employing the categorical approach in the context of §4B1.1. The amendment would change the definitions of a “crime of violence” and a “controlled substance” as they appear in section §4B1.2.

The amendment defines “crime of violence” as the defendant’s own actions, which “the defendant committed, aided or abetted, counseled, commanded, induced, procured, or willfully caused during the commission of the offense, in preparation for that offense, or in the course of attempting to avoid detection or responsibility for that offense.” The amendment also rephrases the language of §4B1.2(a)(1) to include a list of qualifying conduct under a “force clause,” specific named offenses that qualify as a “crime of violence,” as well as a definition of “physical force” that describes a “force capable of causing physical pain or injury to another person.” Such language would be moved from §4B1.2(a)(1) to §4B1.2(b)(1) (A). Under section (b)(2), certain inchoate offenses could now be considered a “crime of violence.” Additionally, the proposed amendment would place the burden of presenting a *prima facie* showing on the Government to classify an offense as a “crime of violence.” These showings would be limited to specific lists of sources of information from the record. All provisions related to the definition of a “crime of violence” would now appear in subsection (b).

The amendment also would exclude state drug offenses from the scope of a “controlled substance offense.” It would instead list specific federal statutes applicable to a “controlled substance offense,” thereby also upholding the current treatment of federal drug trafficking statutes. All provisions related to the definition of a “controlled substance offense” would move from subsection (b) to subsection (a). In addition, the provision that asserts that a violation of 18 U.S.C. § 924(c) or § 929(a) is a “controlled substance offense” if the offense of conviction established that the underlying offense was a “controlled substance offense” would move from the Commentary to subsection (a).

Lastly, the proposed amendment outlines the sentence length qualifications for prior convictions to be considered a “crime of violence” or “controlled substance offense.” The amendment suggests three options. Option 1 would only qualify separately-counted convictions as priors under §4A1.1(a) and §4A1.1(b). Option 2 limits qualifying prior convictions to only those which resulted in a sentence of five years, three years, one year, or more, each of which would count separately under §4A1.1(a) and §4A1.1(b), as well. However, Option 2 also suggests a provision allowing prior convictions to not qualify as a prior felony conviction if the time served in prison was three years, one year, or six months, respectively. Option 3 limits qualifying prior convictions to only those which resulted in having served five years, three years, one year, or more in prison, each of which would count separately under §4A1.1(a) and §4A1.1(b). Under all three options, the amendment provides two sub-options. Sub-option A allows for minimum sentence length requirements to apply to both a “crime of violence” and a controlled substance offense,” while sub-option B only applies said provisions to a “crime of violence.”

Firearms Offenses

Part A of the proposed amendment offers two options to address commenter concerns regarding the insufficient treatment of machinegun conversion devices (MCDs) in §2K2.1. The current statute utilizes two definitions of firearms, with one definition deriving from 21 U.S.C. § 921(a)(3) and the second from 26 U.S.C. § 5845(a). The issue is that only the former includes MCDs.

Option 1 of the proposed amendment would extend the definition of firearms as it applies to §2K2.1 to include all items under 21 U.S.C. § 921(a)(3) and 26 U.S.C. § 5845(a). This option concludes with moving the definition from the Commentary into new subsection (d). Option 2 proposes expanding certain subsections of the current statute to apply to both definitions of firearms under 21 U.S.C. § 921(a)(3) and 26 U.S.C. § 5845(a), where the subsections used to solely apply to the former. The affected subsections are as follows: (b)(1), (b)(4), (b)(5), (b)(6), (b)(7), and (c). Both options would have equivalent results in sentencing.

Part B expands the *mens rea* requirement applied to §2K2.1(b)(4)(B)(ii) in 2023 to all of subsection §2K2.1(b)(4). Hence, a defendant could receive a 2-level enhancement under §2K2.1(b)(4)(A) only if said defendant “knew, was willfully blind to the fact, or consciously avoided knowing that . . . any firearm was stolen.” The same applies to defendants violating §2K2.1(b)(4)(B)(i); said defendants may receive a 4-level enhancement only if they “knew, was willfully blind to the fact, or consciously avoided knowing that . . . any firearm had a serial number that was modified such that the original information is rendered illegible or unrecognizable to the unaided eye.” Such amendments would be addressed in Application Note 8 of the Commentary to §2K2.1 as well.

Circuit Conflicts

The proposed amendment addresses circuit conflicts regarding §2B3.1 (Robbery) and §4A1.2 (Definitions and Instructions for Computing Criminal History), using a two-part approach. Part A and Part B are not mutually exclusive; either could be promulgated with or without the other by the Commission.

Part A seeks to coalesce circuit conflicts regarding the enhancement at §2B3.1(b)(4)(B) for victims “physically restrained” at gunpoint. To resolve whether “physically restrained” applies to victims held at gunpoint but otherwise not restrained by other physical means, the Commission submits three options.

Option 1 would clarify that the enhancement may apply with or without additional physical measures of restraint.⁴ The amendment would add “such as being held at gunpoint or having a path of escape blocked” as an example of physical restraint pertaining to enhancement to §2B3.1(b)(4)(B) alongside the language proposed in Option 2. Option 2 would assert that the physical restraint enhance-

ment only applies to “any person’s freedom of movement was restricted through physical contact or confinement, such as being tied, bound, or locked up, to facilitate commission of the offense or to facilitate escape.”⁵ Option 3 provides a compromise for the circuit conflict by replacing the current physical restraint enhancement with a 2-level enhancement for physical restraints defined by the language in Option 2 as well as a 1-level enhancement for the cases outlined in Option 1.

Part B aims to resolve a circuit conflict in the definition of “intervening arrest” as it applies to counting prior sentences through §4A1.2(a)(2). The amendment responds to circuit concerns by explicitly defining an “intervening arrest” as one that “requires a formal, custodial arrest and is ordinarily indicated by placing someone in police custody as part of a criminal investigation, informing the suspect that the suspect is under arrest, transporting the suspect to the police station, or booking the suspect into jail.”⁶ It further clarifies that a “noncustodial encounter with law enforcement, such as a traffic stop, is not an intervening arrest.”⁷

Simplifying the Three-Step Process

The proposed amendment seeks to restructure the three-step process currently outlined in §1B1.1, with Part A of the amendment identifying issues for comment regarding whether the *Guidelines Manual* should revisit using the three-step process. Furthermore, Part A requests comments surrounding departure and policy statements in relation to specific personal characteristics.

Part B amends the *Guidelines Manual* to better align with court decisions recommending a shift away from using departures and general new requirements for courts. See *United States v. Booker*, 543 U.S. 220 (2005); *Irizarry v. United States*, 553 U.S. 708 (2008). Part B would move the “Original Introduction to the Guidelines Manual” currently in Chapter One, Part A, to the Appendix. Additionally, Part B would revise application instructions of the three-step process in §1B1.1 in two ways. First, the guideline range calculations and the sentencing requirements determination would appear in §1B1.1(a) as the first step in the sentencing process. Second, §1B1.1(b) would contain explicit lists of factors currently outlined for court consideration under 18 U.S.C. § 3553(a).

Moreover, Part B seeks to reconcile statutory limitations and limitations imposed by 18 U.S.C. § 3553(a) to the extent by which courts must consider personal and offense characteristics in sentencing. The provision reassigns §1A1.3 (Authority) as §1A1.1, newly titled “Commission’s Authority.” This new section also would note Congress’ limitations and items not considered as limitations in calculating guidelines to accompany limitations set forth by 28 U.S.C. § 994(a).

Significantly, Part B would delete most instances of “departures” in the *Guidelines Manual*.

All provisions except for those relating to substantial assistance to the authorities and early disposition programs in Chapter Five would be deleted, along with its current title. The Commentary in §1A1.1, §1B1.1, §5B1.1, and §5D1.1 would be amended to reflect these simplifications to the three-step process.

¹ Notice of Amendments to the Local Rules (Published December 1, 2024), <https://www.nced.uscourts.gov/rules/Default.aspx> (last visited July 22, 2025); Federal Rules of Criminal Procedure, <https://www.uscourts.gov/file/78324/download> (last visited July 23, 2025); Federal Rules of Evidence (Published December 1, 2024), <https://www.uscourts.gov/file/78325/download> (last visited July 23, 2025);

² Proposed Amendments to the Federal Rules & Forms (Proposed August 2024), https://www.uscourts.gov/sites/default/files/preliminary_draft_of_proposed_amendments_2024.pdf (last visited July 22, 2025).

³ Proposed 2025 Amendments to the Federal Sentencing Guidelines (Proposed December 19, 2024), https://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/20241230_rf_proposed.pdf (last visited July 22, 2025).

⁴ The First, Fourth, Sixth, Tenth, and Eleventh Circuits promote Option 1.

⁵ The Second, Third, Fifth, Seventh, Ninth, and D.C. Circuits promote Option 2.

⁶ The Third, Sixth, Ninth, and Eleventh Circuits have held a requirement for only official, custodial arrests to qualify as an “intervening arrest” under §4A1.2(a)(2). See *United States v. Ley*, 876 F.3d 103, 109 (3d Cir. 2017); *United States v. Rogers*, 86 F.4th 259, 264-65 (6th Cir. 2023); *United States v. Leal-Felix*, 665 F.3d 1037, 1041 (9th Cir. 2011) (en banc); *United States v. Wright*, 862 F.3d 1265, 1282 (11th Cir. 2017).

⁷ The Seventh Circuit previously contended that a traffic stop qualified as an “intervening arrest.” See *United States v. Morgan*, 354 F.3d 621, 624 (7th Cir. 2003).

The ZA Editors thank Rachel Collins for contributing this helpful information. Rachel was a rising senior undergraduate student at Duke University and was an intern in the FPD office during the summer of 2025.



LOCAL NEWS

Panel News

We are pleased to welcome the following new panel attorneys in Raleigh: Colin Shive; in Greenville: Darren Day; and in Cary: David Saacks.

New to the training panel are the following attorneys in Raleigh: Armina Manning and Jacob Morse; in Wilmington: Dan McCrorie; and in Morehead City: Joseph “Mac” Jennings.

EDNC News

The FPD welcomes newly sworn United States Attorney, W. Ellis Boyle. We extend a warm welcome on behalf of our office and the panel attorneys from this district.

On September 24, 2025, the Court issued Standing Order 25-SO-1 regarding procedures for Access and Management of Sealed Documents, found at <https://www.nced.uscourts.gov/pdfs/StandingOrders/25-SO-1.pdf>. Attorneys are encouraged to review the standing order to familiarize themselves with the new procedures.



If you have a suggestion for an article, we want to hear from you!



Send an e-mail to the Zealous Advocate Editors:

Laura_Wasco@fd.org

or

Vidalia_Patterson@fd.org