SUMMARY
October 3, 2024

2024COA106

No. 22CA0237, *People v. d'Estree* — Constitutional Law — Fourth Amendment — Searches and Seizures — Exclusionary Rule — Independent Source Exception — Inevitable Discovery Exception

A division of the court of appeals reverses the district court's decision declining to suppress evidence obtained from the second of two warrants issued to search the contents of a defendant's cell phone. While the second warrant would have met the independent source doctrine's requirements, here police used an illegally obtained cell phone PIN code to execute the otherwise lawful second warrant. Thus, the district court should have excluded evidence obtained from the phone at trial. The division further holds that when police seek to obtain a cell phone PIN code without a defendant's consent, in this case via a digital "brute force attack," this constitutes a search under the Fourth Amendment and

requires authorization via a warrant. Finally, the division holds that the use of the PIN code here does not meet the requirements of the inevitable discovery doctrine as police abandoned the lawful search to find the PIN code pursuant to the second warrant and expedited their access to the phone using the PIN code illegally obtained pursuant to the first warrant. The defendant's convictions are reversed, and the case is remanded to the district court to hold a new trial.

The special concurrence highlights two aspects of the inevitable discovery jurisprudence that may warrant reconsideration.

COLORADO COURT OF APPEALS **2024COA106**

Court of Appeals No. 22CA0237
Jefferson County District Court No. 19CR4149
Honorable Jeffrey R. Pilkington, Judge

The People of the State of Colorado,

Plaintiff-Appellee,

v.

Alec d'Estree,

Defendant-Appellant.

JUDGMENT REVERSED AND CASE
REMANDED WITH DIRECTIONS

Division II
Opinion by JUDGE FOX
Sullivan, J., concurs
Grove, J., specially concurs

Announced October 3, 2024

Philip J. Weiser, Attorney General, Paul Koehler, Senior Counsel, Denver, Colorado, for Plaintiff-Appellee

Gregory Lansky, Alternate Defense Counsel, Aurora, Colorado, for Defendant-Appellant

¶ 1 Defendant, Alec d'Estree, appeals his convictions, challenging the district court's order declining to suppress evidence gathered from his cell phone using a PIN code obtained via an infirm warrant. We reverse his convictions and remand the case for a new trial.

I. Background

¶ 2 On October 15, 2019, Lakewood police officers responded to a shooting outside an apartment complex around midnight. They found the victim — who had been shot in the chest — in the parking lot. First responders transported him to the hospital, where he later died. A neighbor testified that, shortly before police arrived, she heard arguing, a car horn, and then a gunshot, and saw three individuals rush to a waiting car before driving away. At trial, Autumn Lucero — who had been present when the shooting occurred and accepted a plea deal from the prosecution before she testified — detailed her version of the events leading up to the killing.

¶ 3 Lucero testified that, on October 14, 2019, she was traveling with her ex-boyfriend Manuel Garcia and her cousin Dominic

Maestas.[1] Garcia and Maestas stole several items from a convenience store and later robbed some teenagers in a grocery store parking lot. D'Estree was at Lucero's apartment, to which the group had returned after the robbery. D'Estree joined the group, which then went to a friend's house where Garcia retrieved a silver handgun.

¶ 4 The group next traveled to a private residence in Littleton where, two weeks before, they had sold a stolen iPhone to an individual. According to Lucero, Garcia's sister "had gotten beat up for the stolen iPhone," so the group returned to the residence "to retaliate." Garcia fired the silver handgun at the house "[s]ix or seven times" in a drive-by shooting, but no one was harmed.[2]

¶ 5 Lucero testified that the group still wanted to "make some money" by "robbing, stealing cars, et cetera." While at an apartment complex, Lucero saw d'Estree leave the car with the

---

[1] Lucero, Garcia, and Maestas were originally set to be tried together as codefendants with d'Estree, but the district court later severed d'Estree's trial.

[2] A prosecution expert later testified that her analysis of shell casings and the bullets led her to conclude that the same gun was used in the drive-by shooting and the homicide. A matching shell was also found in Lucero's apartment.

silver handgun before hearing yelling, a car horn, and a gunshot. D'Estree returned to the car and the group left the victim in the parking lot. After arriving home, Lucero photographed Garcia, Maestas, and d'Estree posing with the gun. According to Lucero, the next day d'Estree used his phone to search the internet for "anything about what happened the night before."

¶ 6 The defense pointed out on cross-examination that Lucero's trial testimony substantially differed from her earlier statements to police. For example, in her first interview with police in November 2019, Lucero only told them about the drive-by shooting and not the homicide. During that interview Lucero claimed that only she, Garcia, and Maestas were in the car for the drive-by shooting; at trial, she said that she had initially "forgotten" that d'Estree was there. Lucero further first told police that Garcia forced her, at gunpoint, to drive the car to the drive-by shooting location and that d'Estree later forced her, at gunpoint, to remain in the backseat of the car during the robbery that resulted in the victim's death.

¶ 7 Sergeant Jonathan Holloway testified that the homicide investigation initially produced no suspects, nor did anything connect the drive-by shooting to the homicide, until the police

learned that Garcia wanted to speak to them. Once aware of d'Estree's potential involvement police arrested him, and later charged him on November 14, 2019. Police also seized his Apple iPhone, and searched and downloaded all of its contents after acquiring a search warrant on November 20, 2019.

¶ 8 The district court, however, concluded the first search warrant for the cell phone's contents was invalid because it was overbroad. The prosecution later sought a second warrant to repeat the search, as discussed in greater detail below.

¶ 9 Pursuant to the second warrant, the court allowed police to search the contents of d'Estree's cell phone from October 1, 2019, to November 12, 2019, and the prosecution presented evidence collected from the phone at d'Estree's homicide trial. The prosecution admitted four pictures recovered from d'Estree's phone taken inside Lucero's home approximately one hour after the homicide. One image showed Maestas and d'Estree standing, while d'Estree pointed a silver handgun at the camera. One image showed Garcia smiling for the camera, and another showed Maestas with two handguns, one black and the other silver, tucked

into the strap of what appeared to be a bulletproof vest. The last image showed Garcia pointing both handguns at the camera.

¶ 10 The phone also contained several text messages d'Estree sent in the weeks following the homicide. Most notably, d'Estree sent the following message on November 3, 2019:

> Ayee fam . . . just gotta check in with all my n[*****]s before I get locked up just wanted to let you know I appreciate you fam . . . [.]

¶ 11 The recipient of the message asked when d'Estree would go to prison, and d'Estree responded: "Shit they ain't kaught me yet but they looking for somebody they just won't release the name and shit link soon fam."

¶ 12 Police also recovered d'Estree's internet search history. Holloway testified that police found "[s]earch histories for looking for man shot, articles of man shot in West Denver and Lakewood" from October 15 and 16, 2019.

¶ 13 The jury found d'Estree guilty on all charges — first degree felony murder, second degree murder, conspiracy to commit aggravated robbery, three charges of criminal attempt to commit

aggravated robbery,[3] and two crime of violence sentence enhancers. The district court only sentenced d'Estree for his felony murder and conspiracy to commit aggravated robbery convictions because his second degree murder and attempt to commit aggravated robbery convictions merged into his felony murder conviction. The district court sentenced him to life without the possibility of parole for his felony murder conviction and sixteen years in the custody of the Department of Corrections for the conspiracy to commit aggravated robbery conviction, served concurrently.

¶ 14 This appeal followed. D'Estree raises four main issues, arguing that (1) the district court erred by declining to suppress evidence gathered from his phone after the second warrant was issued; (2) Lucero was coerced into waiving her Fifth Amendment rights and testifying at trial, with the district court improperly advising the jury not to consider Lucero's punishment; (3) the district court erred by failing to properly instruct the jury on

---

[3] The prosecution charged d'Estree with three counts of attempt to commit aggravated robbery under three different theories, but the district court did not require that the prosecution elect a specific theory; rather, it exercised its discretion to simply impose concurrent sentences for each of the theories under which d'Estree was found guilty.

criminal attempt; and (4) given his youth, his sentence to life without the possibility of parole for felony murder is unconstitutional.

¶ 15 We conclude that, in gathering evidence from d'Estree's cell phone, police violated the Fourth Amendment and that no exceptions to the warrant requirement apply, and that the error in allowing the evidence was not harmless beyond a reasonable doubt. We thus reverse his convictions and remand the case for a new trial. We need not address d'Estree's other contentions because they may not arise on retrial. *See People v. Cook*, 197 P.3d 269, 277 (Colo. App. 2008).

II. Phone Search Conducted Pursuant to the Second Warrant

¶ 16 As to the second warrant, d'Estree argues that (1) police's use of the PIN code[4] violated the independent source doctrine because the PIN code was discovered during the first suppressed search and was improperly used in preparing and executing the second warrant; (2) collecting the PIN code through a brute force attack

[4] Where possible, we refer to the specific combination required to access d'Estree's phone as a "PIN code," though we also occasionally refer to "passwords" in a broader sense, and case law and the record occasionally refer to "password" or "pass code."

constituted a search in violation of the Fourth Amendment; and (3) the inevitable discovery doctrine does not apply.

¶ 17 These contentions were preserved. *See People v. Tallent*, 2021 CO 68, ¶ 12; *People v. McFee*, 2016 COA 97, ¶ 31.

A. Additional Background

1. The First Warrant

¶ 18 The challenged cell phone evidence resulted from two separate search warrants, the first of which the court declared invalid. In the first warrant, police requested authorization to search d'Estree's cell phone for the following information:

> 1. *Specialized Location Records:* All call, text and data connection location information, related to all specialized carrier records . . . . Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network. . . .
>
> 2. *Electronically Stored Records:* All records associated with the identified cell phone[], to include all stored communication or files, including voice mail, text messages, including numbers text to and received from and all related content, e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service

> Providers (ISPs), Internet protocol (IP) addresses, (IP) Session data, (IP) Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed), date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with the cell.

A judicial officer approved the first warrant on November 20, 2019, even though the warrant had no subject-matter or date limits.

¶ 19 Dawn Fink, who was admitted as a police expert in "digital forensic analysis" during a pretrial hearing, testified that, in analyzing a cell phone, she typically extracts all electronic information contained on the phone, unless the warrant has constraints. Fink then provides all of the extracted data in a readable format to detectives, who search through the data within the scope of the warrant. The search tools available to her could not first limit the extraction by date.

¶ 20 A return and inventory dated December 18, 2019, detailed that no downloads of d'Estree's phone could yet be completed pursuant to the first warrant because the phone was "password protected." To gain access to the phone, police had earlier reached

out to the United States Secret Service (USSS) in November 2019.[5] Police took d'Estree's phone to the USSS, which installed "Cellebrite," its "advanced tool," on the phone to initiate a "brute force attack." A brute force attack uses a computer program to test every possible combination of a PIN code (here, a six-digit numeric code) until it finds the correct PIN code to access data in the device.

¶ 21 After installing Cellebrite, the USSS returned the phone to local police. Fink testified that police "waited three months or so till [Cellebrite] cracked the code." Fink testified that the timeframe for a brute force attack to test every possible combination for a six-digit PIN code was anywhere from "a week to eleven years."

¶ 22 Once the Cellebrite software discovered the PIN code, Fink returned to the USSS to re-connect the phone to Cellebrite to access the PIN code's digits. With the PIN code in hand, Fink testified that she then extracted all of the information from d'Estree's phone in February 2020, and she provided all the data to detectives.

---

[5] Fink could not specify exactly when in November 2019 police took the phone to the USSS.

¶ 23 D'Estree moved to suppress the results of the first search in March 2021. D'Estree argued that (1) the search occurred without a warrant, as the first warrant did not authorize police to indefinitely hold the phone; (2) the warrant violated Crim. P. 41(d)(5)(VI) and section 16-3-305(6), C.R.S. 2024, because it was executed more than fourteen days after the warrant was issued; and (3) the search was an unlawful general search.

¶ 24 The district court found, in May 2021, that while the warrant was executed beyond the fourteen-day limit, thus violating Crim. P. 41(d)(5)(VI) and section 16-3-305(6), the timing alone did not merit suppression. Relying on *People v. Coke*, 2020 CO 28, ¶¶ 33-38, however, the district court concluded that the warrant lacked sufficient particularly and was a prohibited general warrant. The first warrant "permitted law enforcement to search and seize the entire contents of the [i]Phone; there were no limitations. Notably, there were no subject matter or time limitations on the information to be seized. Such a broad authorization violates the particularity requirement demanded by the Fourth Amendment." Thus, the court suppressed the evidence gathered from the full extraction of d'Estree's phone.

¶ 25 The prosecution next requested that the district court reconsider its ruling, arguing that — even though the warrant lacked a search timeframe — when the warrant was read with the accompanying affidavit, it was sufficiently particular and police acted in good faith. Suppression of this "critical" evidence was therefore unwarranted, the prosecution argued. The district court rejected these arguments.

2. The Second Warrant

¶ 26 With the evidence from the first search suppressed, police sought a second warrant to extract information from d'Estree's cell phone. This time, the warrant specified that it sought information from "October 1, 2019 - November 12, 2019" relating to the homicide. The warrant requested the following information:

- Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
- Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
- Date/time, language, and other settings preferences to include wireless local area

network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;

- System and device usage files, logs, and databases utilized to record device activities such as lock/unlock activities, powering on/off cycles, installation and deletions records;

- Telephone contact lists, phone books and telephone logs;

- Data contained in notes, reminders, documents, calendars and/or other similar applications that relates to the planning and commission of the attempt[ed] Homicide/ Homicide that occurred between October 1, 2019 - November 12, 2019;

- Communications made, stored, sent, received or deleted that relate to the planning and commission of the attempt[ed] Homicide/Homicide that occurred between October 1, 2019 - November 12, 2019;

- Photos and videos created, stored, sent, received or deleted, or documents containing such photographs or videos that relate to the planning and commission of the attempt[ed] Homicide/Homicide that occurred between October 1, 2019 - November 12, 2019;

- All electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media and

third-party applications located on the device that relate to the planning and commission of the attempt[ed] Homicide/ Homicide that occurred between October 1, 2019 - November 12, 2019;

- Communications through the SIRI/(GOOGLE ASSISTANT system[)], including all communications entered and/or recorded into the system as well as communicated from the system to the user that relate to the attempt[ed] Homicide/ Homicide that occurred between October 1, 2019 – November 12, 2019;

- Global position system (GPS) data and any other geolocation data that relates to the planning and commission of the attempt[ed] Homicide/Homicide that occurred between October 1, 2019 - November 12, 2019;

- Records of internet activity that relates to the planning and commission of the attempt[ed] Homicide/Homicide that occurred between October 1, 2019- November 12, 2019, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses pertaining to violations of the law or that show who used, owned, possessed, or controlled the device(s).

The district court approved the second warrant on October 11, 2021. After d'Estree's arrest, the phone had remained in police custody (except for the brief times the USSS handled it).

¶ 27 Fink conducted the second extraction seeking to collect all information from the phone, without limitation, to ensure no relevant information was missed, but this time she provided the detectives only data within the dates specified in the warrant. Fink also explained that a new tool available after the first warrant, "GrayKey," was used to conduct the extraction, which allowed police to conduct three types of extractions: a "partial BFU" (before first unlock), an "instant AFU" (after first unlock), or a "full-file system" AFU extraction. Fink testified that a partial BFU extraction "provides generally just system data," and occasionally some photos, and is used "to see if there's any information to potentially find [PIN] codes for the device." This type of extraction is the only extraction available without a PIN code. Having a PIN code enables conducting an AFU extraction, with the "full-file system" AFU providing all information on a device, but it could take years to crack the PIN code.

¶ 28 Fink conducted a BFU extraction on October 12, 2021, and then initiated a brute force attack. Fink allowed the program to run for seven days without success; then she abandoned the brute force attack in favor of expediting the process by using a six-digit code she found on the back of the phone — d'Estree's PIN code — to unlock the phone and conduct the AFU.[6] It is unclear exactly how the PIN code came to be adhered to the phone after the first search — there is no evidence indicating that the PIN code was originally there — and Fink conceded that the USSS "could have" placed the code there.

¶ 29 Once the PIN code unlocked the phone on October 18, Fink conducted a full-file system AFU extraction with GrayKey, downloaded the phone's contents, and then used Cellebrite to "decode" the raw data. Once decoded, Fink used Cellebrite to select only data from October 1 to November 12, 2019 (the range specified

---

[6] Fink testified that she tried birthdates and the PIN code on the phone as these numbers were "suggested" to her after the first seven days of the brute force attack proved unsuccessful. There is no evidence in the record that the PIN code changed between the first and second searches, so we assume that the PIN code Fink used is the same one that police used to first access the phone.

in the warrant), and provided this information to police in a "user-friendly" report.

¶ 30 Holloway testified that, when drafting the second warrant application and affidavit, he relied on information "[f]rom the first warrant" but did not place any information learned from the suppressed search into the second warrant application. Beyond limiting the scope to specific dates, the "only thing that was added [was] . . . some explanations of cell phone capabilities."

¶ 31 D'Estree challenged the second warrant, arguing that it (1) was not independent of the first warrant's illegality; (2) relied on suppressed evidence, including the PIN code; and (3) did not cabin the police's search, which also exceeded the warrant's legitimate scope. Allowing this evidence would also be unfair, d'Estree argued.

¶ 32 The district court declined to suppress the cell phone evidence gathered pursuant to the second warrant.

¶ 33 The district court found that police sought the second warrant for reasons independent of information learned from the first, thus meeting the "independent source doctrine" criteria. It noted that

> [t]he Second Affidavit was essentially the same as the First Affidavit with three exceptions: (1) a reference to the court's prior suppression

> orders; (2) an expanded explanation of cellphone capabilities; and (3) inclusion of the Second Date Range. Of significance here, nothing in the Second Affidavit referenced the information seized in the February Search.

It also found that Holloway's testimony — that he did not rely on information from the first suppressed search — was credible and noted that there was no contrary evidence.

¶ 34 Regarding use of the PIN code (found on the back of the phone), the district court said that suppression was unwarranted for two reasons. First, the district court concluded that the retrieval of the PIN code through a brute force attack during execution of the first warrant did not constitute a Fourth Amendment search. Recognizing that there were no Colorado cases on the issue, it analogized to how police officers execute search warrants against a locked house. Police may break into a home to execute a search warrant and the actual breach of the home — via a door or through a window — is not a search; rather, it is a "means" to conduct a search.

¶ 35 The court also found that the discovery of the PIN code fell within the "inevitable discovery" exception to the exclusionary rule, noting that, "[e]ven though it was listed on the back of the

cellphone[,] . . . if it had not been available, law enforcement would have obtained it through the [USSS] or its own software." It also noted that case law "has not distinguished between evidence that would have been discovered quickly and evidence that would have taken much longer to discover." Thus, because the PIN code would have been revealed once all possible combinations were tested, there was a "reasonable probability" — indeed, the court found, because there was a finite number of possible combinations, there was a "100% probability" — that the PIN would have been discovered eventually. The district court rejected the defense's fairness argument as unsupported by case law.

B. Standard of Review and Applicable Law

¶ 36 "Whether evidence should be suppressed is a mixed question of law and fact. As a result, we defer to the trial court's factual findings if they are supported by competent evidence, but we review the legal effect of those findings de novo." *People v. Seymour*, 2023 CO 53, ¶ 19 (citation omitted).

¶ 37 "The United States and Colorado Constitutions protect individuals against 'unreasonable searches and seizures.'" *Id.* at ¶ 20 (quoting U.S. Const. amend. IV; Colo. Const. art. II, § 7). A

"search" within the meaning of the Fourth Amendment "occurs when the government infringes on an individual's reasonable expectation of privacy." *Id.* (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan J., concurring)). The "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *Id.* (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). "[T]o deter police misconduct" and discourage illegal searches, "the exclusionary rule requires courts to suppress evidence at trial if the government acquired it in violation of constitutional protections."[7] *Id.* at ¶ 62.

¶ 38 A warrant is generally required before cell phone data can be searched. *See Riley v. California*, 573 U.S. 373, 386, 393-98, 401-403 (2014) (recognizing the ubiquity of cell phones, their immense storage capacity, and their potential to store deeply personal information). Our state supreme court has also "acknowledged the special protections applicable to cell phone searches." *People v.*

---

[7] The exclusionary rule "applies both to illegally obtained evidence and to derivative evidence — often called 'fruit of the poisonous tree.'" *People v. Dominguez-Castor*, 2020 COA 1, ¶ 19 (quoting *People v. Schoondermark*, 759 P.2d 715, 718 (Colo. 1988)).

Davis, 2019 CO 24, ¶ 19; *see also Coke*, ¶ 38 (warrant to search a cell phone that "permitted the officers to search all texts, videos, pictures, contact lists, phone records, and any data that showed ownership or possession" violated the Fourth Amendment's particularity requirement). Indeed, "the general trend of caselaw provides cell phones with more protection, not less." *Davis*, ¶ 17.

¶ 39 Preserved errors concerning the admission of evidence in violation of the Fourth Amendment implicate "trial errors of constitutional dimension," and thus we review any such error for "constitutional harmless error." *Hagos v. People*, 2012 CO 63, ¶ 11. "These errors require reversal unless the reviewing court is 'able to declare a belief that [the error] was harmless beyond a reasonable doubt.'" *Id.* (alteration in original) (quoting *Chapman v. California*, 386 U.S. 18, 24 (1967)).

C. Analysis

1. The Independent Source Doctrine

¶ 40 The independent source doctrine is an exception to the exclusionary rule and allows "unconstitutionally obtained evidence [to] be admitted if the prosecution can establish that it was also discovered by means independent of the illegality." *People v.*

Dominguez-Castor, 2020 COA 1, ¶ 20 (quoting *People v. Arapu*, 2012 CO 42, ¶ 29); *see also People v. Thompson*, 2021 CO 15, ¶ 21. The doctrine may apply to "evidence seized under a valid warrant issued after the evidence was first discovered during execution of an invalid warrant . . . if the prosecution shows that the second warrant was truly independent of information obtained from the initial search." *Dominguez-Castor*, ¶ 22. The decision to seek an additional warrant because of a suppression order's consequences does not, on its own, violate the independent source doctrine. *People v. George*, 2017 COA 75, ¶ 55.

¶ 41 A second warrant meets the criteria of the independent source doctrine if the prosecution proves, by a preponderance of the evidence, that "(1) the decision to seek the warrant was not prompted by what was observed during the initial unlawful search, and (2) no information obtained during the initial search was relied upon by the magistrate in issuing the warrant." *Dominguez-Castor*, ¶ 21; *see also Thompson*, ¶ 22. It is a question of fact for the district court "[w]hether the police would have pursued a second search even absent what they discovered during an earlier unlawful

search . . . . We will not disturb the court's finding if it has record support." *Dominguez-Castor*, ¶ 34.

¶ 42 The reasoning behind the independent source doctrine, articulated in *Nix v. Williams*, is that

> the interest of society in deterring unlawful police conduct and the public interest in having juries receive all probative evidence of a crime are properly balanced by putting the police *in the same, not a worse, position that they would have been in if no police error or misconduct had occurred*. When the challenged evidence has an independent source, exclusion of such evidence would put the police in a worse position than they would have been in absent any error or violation.

467 U.S. 431, 443 (1984) (emphasis added) (citations and footnote omitted). Put another way, "while the government should not profit from its illegal activity, neither should it be placed in a worse position than it would otherwise have occupied." *Murray v. United States*, 487 U.S. 533, 542 (1988).

¶ 43 The district court deemed Holloway's testimony — averring that the information from the first suppressed search did not inform the second warrant application or the decision to seek the second warrant — credible. *See Dominguez-Castor*, ¶ 21. We may not disturb this credibility determination. *See Seymour*, ¶ 20. Nor does

the second warrant reference information learned during the first search on which a judicial officer could have improperly relied. *See Dominguez-Castor*, ¶ 21.

¶ 44 But d'Estree challenges the independence of the second warrant because he argues it sought information that police had discovered during the first search and knew existed. Therefore, he contends the second warrant relied on information illegally obtained in the first search. For example, d'Estree points to the second warrant's request for information on any "search terms that the user entered into any internet search engine" as problematic. D'Estree argues that the object of this request was to gather his known internet search history (which was introduced at trial), and improperly relied on information gathered in the first search.

¶ 45 But the first warrant request, while not as specific, requested such information when it sought "web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, [and] (IP) Session data." The second warrant's request with additional specificity does not necessarily show that the second warrant relied on information improperly gained from the

first search. *See id.* at ¶ 14 & n.2 (second warrant contained "much more information than the first" in light of police's increased training on search warrants for cell phones).

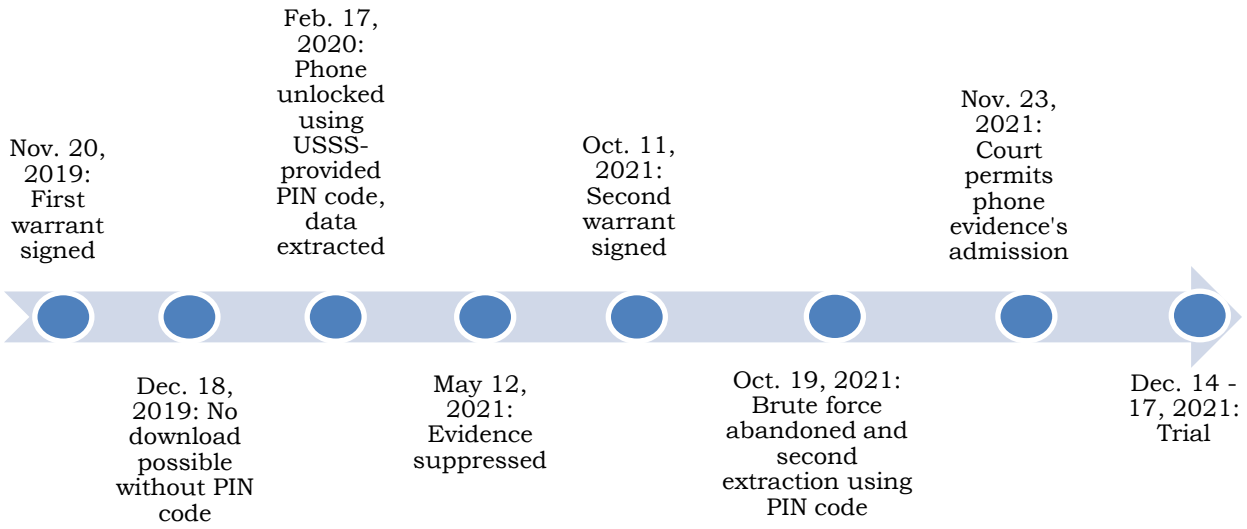
¶ 46 As a result, the second warrant itself meets the criteria detailed in *Dominguez-Castor* for the independent source doctrine exception. Had police relied on the second warrant alone to retrieve the contents of d'Estree's cell phone, that would have been permissible and the extracted evidence would have been properly admitted at trial. But police used illegally obtained information from the first warrant — the PIN code — in *executing* the second warrant.

2. The Use of the PIN Code

¶ 47 The PIN code was discovered during the execution of the first, unlawful general warrant. Police then used this illegally obtained information to *expedite* the execution of the second warrant. By using the illegally obtained PIN code, police extracted a crucial benefit — guaranteed access to the phone's contents ahead of the forthcoming December 2021 trial. This conduct placed the government in a better position than before the illegal search occurred. *See Murray*, 487 U.S. at 542; *Nix*, 467 U.S. at 443. So

while the second warrant was not infirm, the execution of that warrant most certainly was.

¶ 48 A summary of the key dates relating to both warrants follows:



Key Warrant Events

¶ 49 Police and the prosecution had months to submit another warrant application after the first warrant was invalidated, and could have done so, but they did not request a second warrant until about two months before trial. The first brute force attack took three months, and Fink testified that a brute force attack could have taken up to eleven years, so there was no guarantee that

police would have gained access to the phone in time for trial *without* relying on the illegally obtained shortcut (the PIN code).[8]

¶ 50 As the United States Supreme Court held in *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920), which originated the independent source doctrine, "[t]he essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court *but that it shall not be used at all*." (Emphasis added.)

¶ 51 The second warrant authorized police to acquire the PIN code via brute force attack; evidence on the phone so acquired would have presumably met the independent source doctrine. *See Dominguez-Castor*, ¶ 21. However, police abandoned the brute force attack and, instead, took a different (and shorter) route to the encrypted information using illegally obtained information (the PIN code) to *execute* the second warrant. Law enforcement may not use information obtained in violation of the Fourth Amendment. *See*

---

[8] If the prosecution had pursued the second warrant immediately after the information obtained with the first warrant was suppressed in May 2021, even if it took three months (as it had before) to unlock the phone, there may have been substantially less incentive to use the PIN code to expedite access to the phone's contents before the December 14, 2021, trial start date.

Silverthorne, 251 U.S. at 392. With this framework in mind, we proceed to address the district court's other grounds for admitting the evidence.

3. Whether a Brute Force Attack Constitutes a Search

¶ 52 The district court also found that the use of a brute force attack to discover a PIN code and access d'Estree's cell phone data did not constitute a search under the Fourth Amendment because it was a "means" to execute a warrant rather than a search. It analogized the issue as akin to when police execute a warrant to search a locked house — whether police choose to enter through the door or a window is irrelevant.

¶ 53 Case law supports this general concept — most notably, as pointed out by the district court and the People on appeal, in *Dalia v. United States*, 441 U.S. 238 (1979). There, a defendant challenged a wiretap order granting the government the authority to "intercept all oral communications taking place in petitioner's office" through electronic surveillance. *Id.* at 241-42. The defendant argued that the order violated the Fourth Amendment because it did not specify the means used to execute the warrant (i.e., by covert entry into the office). *Id.* at 256-58. The Supreme Court held

that "[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed." *Id.* at 257. Instead, the means of executing a warrant are "generally left to the discretion of the executing officers . . . subject of course to the general Fourth Amendment protection . . . [, and] the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Id.* at 257-58.

¶ 54 But the means versus search distinction does not neatly fit here. As the United States Supreme Court aptly recognized in *Riley v. California*, analogizing the digital world and processes to the physical world is difficult and unhelpful, and "[a]n analogue test would 'keep defendants and judges guessing for years to come.'" 573 U.S. at 401 (citation omitted). The use of a brute force attack to access a phone, or any other means to obtain a phone's PIN code without a defendant's cooperation or consent, is fundamentally different from entry into a home with a warrant because a search for the PIN code itself, just like a search of a cell phone's contents, is protected by the Fourth Amendment. *See Davis*, ¶ 19; *Coke*,

¶ 38; *Riley*, 573 U.S. at 386, 393-98, 401-03 (recognizing that cell phones hold "the privacies of life" (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886))).

¶ 55 While the protections the Fourth Amendment affords to passwords and PIN codes allowing access to cell phones are less clearly defined than those it affords to physical spaces and the personal data cell phones contain,[9] existing Fourth Amendment principles, coupled with the recognition of the special protections afforded cell phones, support concluding that obtaining a cell phone PIN code without consent requires a warrant. *See United States v. Booker*, 561 F. Supp. 3d 924, 929-32 (S.D. Cal. 2021) (holding, in part, that requiring defendant to involuntarily enter his PIN code while law enforcement watched and recorded it, before police sought a warrant to search the phone using software that required the PIN code, violated the Fourth Amendment).

---

[9] The issues in this case are distinct from those in the Fifth Amendment context centering on whether a defendant can be compelled to provide a cell phone PIN code or unlock a device. *See, e.g.*, *Seo v. State*, 148 N.E.3d 952, 962 (Ind. 2020) (holding that forcing a defendant to "unlock her iPhone for law enforcement would violate her Fifth Amendment right against self-incrimination"). The Fifth Amendment is not at issue in this case.

¶ 56 Courts use "a two-prong test to determine if a claimed privacy interest warrants constitutional protection: (1) whether the individual 'exhibited an actual (subjective) expectation of privacy' and (2) whether, objectively, 'the expectation [is] one that society is prepared to recognize as 'reasonable.'" *Seymour*, ¶ 22 (quoting *People v. Gutierrez*, 222 P.3d 925, 932 (Colo. 2009), in turn citing *Katz*, 389 U.S. at 361).

¶ 57 Turning to the subjective expectation of privacy prong, there is no evidence that d'Estree exhibited anything other than an expectation that his PIN code would remain private. This is evidenced by the very fact that police had to use specialized software to break into the phone because d'Estree did not provide the PIN code. On this point, *Davis*, 2019 CO 24, provides some insight. There, the Colorado Supreme Court held that an individual who voluntarily gave his phone's PIN code to law enforcement — even for a limited purpose — "had no legitimate expectation of privacy in the digits of his passcode" and "law enforcement's [later] use of that passcode was not a search protected by the Fourth Amendment." *Id.* at ¶¶ 30-32. It stands to reason, therefore, that when an individual does *not* voluntarily share a PIN code with

police, he is exhibiting a subjective expectation that his PIN code will remain private — particularly when a phone's PIN code is the key to unlocking a wealth of private information.

¶ 58 As for the second, objective prong, it is clear that society recognizes as reasonable the expectation that one's PIN code is private. Indeed, keeping a PIN code private is an indisputably important part of how passwords function. *See Booker*, 561 F. Supp. 3d at 931 ("There can be no question that a passcode entered into a cell phone, which is designed to keep the contents of the phone hidden from others, is generally considered by society to be something private that should be free from warrantless intrusion by the government."); *see also* Jay E. Grenig, *Electronic Discovery and Records and Information Management Guide* § 3:7, Westlaw (database updated Oct. 2023) ("It is essential to use passwords and to keep them safe. . . . No one else should be told a password. Any compromised password should be changed immediately."); *Davis*, ¶ 30 (society would not deem a subjective expectation of privacy to be objectively reasonable *if* a defendant shared the PIN code with law enforcement).

¶ 59 The People contend that d'Estree's PIN code "had no meaningful existence other than to protect the contents of his cellphone — it was just a series of numbers that provided no independent information about his thoughts or life." This is true in the most literal sense of what a PIN code is. But this characterization of a PIN code ignores the importance of what a phone's PIN code protects — namely, the wealth of private information cell phones store. *See Riley*, 573 U.S. at 393-94, 401-03.

¶ 60 Because d'Estree has a cognizable right to the privacy of his cell phone PIN code that warrants constitutional protection under the subjective and objective prongs of the *Katz* test, we conclude a brute force attack to discover d'Estree's PIN code constitutes a search under the Fourth Amendment. The second warrant allowed police to obtain "[p]asswords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents." A brute force attack was therefore authorized. But the use of the PIN code discovered while executing the first, invalid warrant was not authorized. The district court's "means" rationale therefore cannot save the execution of the second warrant

using the PIN code discovered while executing the first, unlawful warrant. *See Riley*, 573 U.S. at 400; *Dominguez-Castor*, ¶ 19.

4. The Inevitable Discovery Rule

¶ 61 "Under the inevitable discovery rule, evidence initially discovered in an unconstitutional manner may be received if that same evidence inevitably would have been obtained lawfully." *People v. Schoondermark*, 759 P.2d 715, 718 (Colo. 1988). "The ability to obtain a lawful search warrant after an illegal search has occurred does not satisfy the inevitable discovery exception requirements." *People v. Nelson*, 2012 COA 37, ¶ 52; *see also People v. Diaz*, 53 P.3d 1171, 1176 (Colo. 2002).

> The Government cannot later initiate a lawful avenue of obtaining the evidence and then claim that it should be admitted because its discovery was inevitable. . . . Because a valid search warrant nearly always can be obtained after the search has occurred, a contrary holding would practically destroy the requirement that a warrant for the search . . . be obtained *before* the search takes place.

People v. Burola, 848 P.2d 958, 963-64 (Colo. 1993) (quoting *United States v. Satterfield*, 743 F.2d 827, 846 (11th Cir. 1984)). As a result, "[t]he prosecution must affirmatively show that the lawful means of discovering this evidence was already initiated when the

evidence was obtained illegally." *People v. Dyer*, 2019 COA 161, ¶ 38.[10]

¶ 62 As with the independent source doctrine, this requirement effectuates the policy underlying the inevitable discovery doctrine — the exception should place the government in the *same* position (no better, no worse) than it would have occupied if no illegality had occurred. *See Nix*, 467 U.S. at 443-44 (the independent source doctrine's "rationale is wholly consistent with and justifies our adoption of the ultimate or inevitable discovery exception to the exclusionary rule"). Thus, if two searches — one lawful and one unlawful — began at the same time and would procure the same evidence, suppressing the resulting evidence would place the prosecution in a worse position because the police would have inevitably obtained that evidence even if no misconduct had taken place. *Id.*

¶ 63 While it is true, as the district court noted, that the PIN code would have eventually been discovered by police software — months

---

[10] Some courts, including the Tenth Circuit, do not require the lawful means of discovering the evidence to have been initiated before the unlawful search or seizure. *See, e.g.*, *United States v. Christy*, 739 F.3d 534, 540-41 (10th Cir. 2014).

or years later — focusing on the word "inevitable" in such a manner ignores the requirements of the rule and undermines its purpose, and the exclusionary rule more broadly.[11] While police here initiated a *lawful* means to obtain the PIN code — via the brute force attack that the second warrant authorized — that means was abandoned in favor of a shortcut (using the illegally obtained PIN code), thus violating a key requirement of the inevitable discovery rule under Colorado precedent. *See Dyer*, ¶ 38; *Nelson*, ¶ 52. And regardless, the soon-abandoned lawful means was initiated well after the PIN code was first illegally obtained. *See Dyer*, ¶ 38. Simply because police software would have *eventually* discovered the PIN code (perhaps years after d'Estree's trial date) does not render it admissible.

¶ 64 Even if we assume the second brute force attack would have yielded a PIN code in three or so months (the time the first brute

---

[11] Merriam-Webster's Dictionary defines "inevitable" as "incapable of being avoided or evaded." Merriam-Webster Dictionary, https://perma.cc/B3BN-X46N. Black's Law Dictionary defines "inevitable" within the context of the inevitable discovery rule. In that definition, it notes that "[t]he inevitable discovery of evidence by law enforcement is a discovery that would naturally and lawfully occur in the course of an investigation." Black's Law Dictionary 925 (12th ed. 2024).

force attack took using the first, unlawful warrant), the information would likely have come *after* the scheduled December 14, 2021, trial. We are not prepared to speculate that the district court would have granted a trial continuance when the prosecution waited so close to the trial date to seek a second warrant. *See People v. Syrie*, 101 P.3d 219, 223 (Colo. 2004) (inevitable discovery exception cannot be met through "speculation about possible series of events"). Recall that police asked the court for the second warrant in October 2021 — almost five months after the May 12, 2021, suppression ruling — knowing that d'Estree's trial was in December 2021 and his speedy trial clock was ticking.

¶ 65 To admit evidence under the inevitable discovery doctrine "requires an affirmative showing of a reasonable probability that the evidence *would inevitably be discovered through lawful means already initiated when the seizure was made*." *Id.* (emphasis added); *see also Burola*, 848 P.2d at 963 ("[I]f evidence is obtained by illegal conduct, the illegality can be cured only if the police possessed and were pursuing a lawful means of discovery at the time the illegality occurred."). A lawful means was initiated — the brute force attack authorized by the second warrant — but that

means was abandoned in favor of using the proverbial fruit of the first, poisoned warrant — the known PIN code.

¶ 66 The primary rationale for the inevitable discovery rule as an exception to the exclusionary rule would be undermined by allowing admission of any evidence that would have been eventually discovered, where a lawful means to obtain the evidence was initiated but abandoned in favor of a tainted shortcut. *See Nix*, 467 U.S. at 442-43; *see also Casillas v. People*, 2018 CO 78M, ¶¶ 21-22, 36.

¶ 67 We recognize that the exclusionary rule's deterrence rationale is not served when the challenged evidence would "ultimately or inevitably" be discovered by lawful means. *Nix*, 467 U.S. at 444 ("If the prosecution can establish . . . that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received."). As the *Nix* court reasoned, "when an officer is aware that the evidence will inevitably be discovered, he will try to avoid engaging in any questionable practice . . . [as] there will be little to gain from taking any dubious 'shortcuts' to obtain the evidence." *Id.* at 445-46; *see also People v. Briggs*, 709 P.2d 911, 923 (Colo.

1985). But here, the opposite occurred — police took a shortcut, presumably because they were not confident that the second brute force attack would crack the cell phone in time to put its incriminating contents to use at the December 2021 trial.

¶ 68 To rule that use of the PIN code was permissible in this context would provide an incentive for police to engage in such shortcuts in the future. *See Casillas*, ¶¶ 34-36. Although there is a reasonable probability that police software would have *eventually* produced d'Estree's PIN code, by Fink's own estimates and prior brute force attack, we can only speculate whether this would have occurred before the December 2021 trial. *See Syrie*, 101 P.3d at 223.

D. Prejudice and Next Steps

¶ 69 In their brief, the People "concede that if this Court where [sic] to find that the trial court erred in denying all of [d'E]stree's preserved suppression claims, under the facts of this case, the errors could not be harmless." We agree.

¶ 70 The admission of the evidence gathered from d'Estree's cell phone undoubtedly prejudiced him at trial. Photos of d'Estree holding a handgun that matched the description of the homicide

weapon, text messages admitting that he expected to go to prison, and the incriminating internet search history were impactful pieces of evidence against d'Estree. Further, the prosecutor referred to this evidence several times in closing argument, pointing to it to help convince the jurors that, regardless of what they thought of Lucero's credibility, they could rely on the evidence taken from d'Estree's cell phone to corroborate her testimony. And the prosecution noted in its motion for reconsideration after the first warrant's suppression that it considered the "evidence collected from the cell phone belonging to the defendant [to be] of critical importance to the prosecution of this case."

¶ 71 We cannot find that the improper admission of this critical evidence against d'Estree was harmless beyond a reasonable doubt. Furthermore, these errors likely impacted every one of his convictions. The prosecution's trial evidence supporting each of d'Estree's convictions, especially Lucero's testimony, benefited from this improperly admitted digital evidence for corroboration. Thus,

these errors require reversal of each of his convictions.[12] *See Hagos*, ¶ 11; *see also People v. Folsom*, 2017 COA 146M, ¶¶ 17-23 (admission of videos extracted from iPod was not harmless and required reversal).

¶ 72 In the light most favorable to the prosecution, however, considering both the properly admitted evidence through witness testimony and the police's investigation, in addition to the improperly admitted cell phone evidence, we cannot say with certainty that there was insufficient evidence to convict d'Estree of some or all of the charged crimes. And because this reversal is predicated on the receipt of improperly admitted evidence, the prosecution is entitled to a retrial of all of d'Estree's charges on remand. *See People v. Marciano*, 2014 COA 92M-2, ¶¶ 42-49; *see also People v. Sisneros*, 606 P.2d 1317, 1319 (Colo. App. 1980) ("[W]here reversal is predicated upon trial error consisting of the reception of inadmissible evidence, remand for a new trial is proper,

---

[12] The People do not address whether any of d'Estree's convictions may have been unaffected by the admission of the digital evidence were we to find the execution of the second warrant was infirm, while d'Estree contends that every one of his convictions must be reversed.

and an appellate court should not review the remaining evidence in order to determine whether it is sufficient to sustain the conviction.") (citations omitted).

III. Disposition

¶ 73 We reverse d'Estree's convictions and remand the case to the district court for a new trial.

JUDGE SULLIVAN concurs.

JUDGE GROVE specially concurs.

JUDGE GROVE, specially concurring.

¶ 74 I agree with the majority's reasoning and its conclusion that d'Estree's convictions must be reversed. I write separately to urge the Colorado Supreme Court to revisit two aspects of its inevitable discovery jurisprudence that I believe have drifted away from the United States Supreme Court's articulation of the rule.

¶ 75 First, since the doctrine was first applied in this state, Colorado's version of the inevitable discovery rule has required the prosecution to show that (1) "the police were pursuing an independent investigation at the time the illegality occurred," and (2) there was "*a reasonable probability* that the evidence would have been discovered in the absence of police misconduct." *People v. Breidenbach*, 875 P.2d 879, 889 (Colo. 1994) (emphasis added). My concern in this case is with the second element of this test, which not only makes little semantic sense but also materially diverges from the standard set forth in *Nix v. Williams*, 467 U.S. 431 (1984).

¶ 76 *Breidenbach*'s "reasonable probability" approach tracked the Fifth Circuit Court of Appeals' holding in *United States v. Cherry*, 759 F.2d 1196 (5th Cir. 1985), which applied pre-existing circuit precedent to define the scope of the inevitable discovery rule based

on its conclusion that the *Nix* court had made "no attempt . . . to define the contours of that exception." *Id.* at 1204. But however thin the analysis in *Nix* may have been, it still clearly held that the inevitable discovery rule only applies if the prosecution "establish[es] *by a preponderance of the evidence* that the information ultimately or inevitably would have been discovered by lawful means." *Nix*, 467 U.S. at 444 (emphasis added).[1] The preponderance standard is different from "reasonable probability," and, importantly for this case, it also places a heavier burden on the prosecution. *See United States v. Zavala*, 541 F.3d 562, 579 n.7 (5th Cir. 2008) (acknowledging that the Fifth Circuit's application of the "reasonable probability" test rather than a preponderance standard in the context of the inevitable discovery rule "is more favorable to the Government than the test in other circuits"); *cf. Mile High Cab, Inc. v. Colo. Pub. Utils. Comm'n*, 2013 CO 26, ¶ 15

[1] I recognize the linguistic difficulties in measuring inevitability in terms of probability. *See, e.g.*, *United States v. Cabassa*, 62 F.3d 470, 474 (2d Cir. 1995) (recognizing the "semantic puzzle" created by "using the preponderance of the evidence standard to prove inevitability"). But that standard is dictated by the holding in *Nix v. Williams*, 467 U.S. 431 (1984), and has generally proved workable in the context of suppression rulings.

(observing that "reasonable probability" is used "to refer to a likelihood of occurrence which, although not insignificant, nevertheless need not rise to the level of a preponderance of the evidence"); *Krutsinger v. People*, 219 P.3d 1054, 1060 (Colo. 2009) ("[T]he Supreme Court has made abundantly clear that it does not intend its use of the term 'reasonable probability' to require a showing that the defendant would more likely than not have received a different result . . . ."). As a result, Colorado's version of the inevitable discovery rule appears to be out of step with Supreme Court precedent.[2]

¶ 77 To be sure, in practice it will often make no difference whether the "reasonable probability" or preponderance standard applies.

---

[2] Notably, the Colorado Supreme Court's application of the "reasonable probability" test in inevitable discovery cases also diverges from its application of a preponderance standard in the closely related context of the independent source doctrine. *See People v. Thompson*, 2021 CO 15, ¶ 22 ("When, as here, the People assert the applicability of the independent source doctrine, they bear the burden of proving by a preponderance of the evidence the doctrine's applicability."). Because the two exceptions share the same doctrinal underpinnings, *see Murray v. United States*, 487 U.S. 533, 539 (1988) (observing that "[t]he inevitable discovery doctrine . . . is in reality an extrapolation from the independent source doctrine"), I see no reason why the same standard should not apply to both.

But in close cases, the test that the trial court applies may well be dispositive. This case provides a perfect example. Given that the United States Secret Service took three months to complete a brute force attack on the phone's PIN code, I believe that it was reasonably probable that a second brute force attack would also be successful within a similar amount of time. But I am far less certain that the prosecution *proved by a preponderance of the evidence* that cracking the PIN code would be inevitable in any sort of reasonable timeframe. *See United States v. Jones*, 72 F.3d 1324, 1334 (7th Cir. 1995) ("Inevitable discovery is not an exception to be invoked casually, and if it is to be prevented from swallowing the Fourth Amendment and the exclusionary rule, courts must take care to hold the government to its burden of proof."). To the contrary, the only evidence on this point was Agent Fink's testimony that, if she had not decided to use the illegally obtained PIN code after only a week of searching, the brute force attack could have taken "anywhere from a week to 11 years" to unlock the phone. Fink offered few other details about how quickly the process was likely to proceed or how the software worked. Information of that sort would have helped the court better assess how the search

would turn out. For example, if the court had been presented with evidence that the software attempts easy-to-remember PIN codes (like the one here) first, before moving on to more random numbers, it might have been able to better forecast the likelihood that execution of the second warrant would have been successful in the time remaining before trial.

¶ 78 I acknowledge that the prosecution could have sought up to a six-month continuance of the trial date if it had tried and failed to discover the PIN code. *See* § 18-1-405(6)(g)(I), C.R.S. 2024. But in light of Fink's testimony, it appears that an extension of that length would have offered little additional certainty and might, depending on the overall age of the case, have begun to raise constitutional speedy trial concerns. *See People v. Nelson*, 2014 COA 165, ¶¶ 21-25. Accordingly, if the district court had been required to hold the prosecution to the burden of proof dictated by *Nix*, it might well have granted d'Estree's motion to suppress.

¶ 79 Second, in my view, parties and trial courts in Colorado would be well served by an approach to the inevitable discovery doctrine that explicitly takes deterrence into account. I do not mean to suggest that the prosecution should be required to show an

absence of bad faith (indeed, *Nix* rejected that very argument, 467 U.S. at 445), but as Justice Stevens pointed out in his *Nix* concurrence, the inevitable discovery doctrine would "be inconsistent with the deterrent purposes of the exclusionary rule" if it provided law enforcement with an incentive to commit constitutional violations "by permitting the prosecution to avoid the uncertainties inherent in its search for evidence." *Id.* at 456 (Stevens, J., concurring in the judgment). Consistent with this understanding, some federal circuits have made clear that the inevitable discovery exception should not apply under circumstances that would undermine the fundamental purpose of the exclusionary rule. *See, e.g.*, *United States v. Crespo-Rios*, 645 F.3d 37, 42 (1st Cir. 2011) (holding that inevitable discovery should apply only where "application of the doctrine in a particular case will not sully the prophylaxis of the Fourth Amendment" (quoting *United States v. Hughes*, 640 F.3d 428, 440 (1st Cir. 2011))); *United States v. Vasquez De Reyes*, 149 F.3d 192, 195 (3d Cir. 1998) (holding that the inevitable discovery rule "permits the court to balance the public interest in providing a jury with all relevant and

probative evidence in a criminal proceeding against society's interest in deterring unlawful police conduct").[3]

¶ 80 As the majority's analysis makes clear, the circumstances before us here seem to be exactly what those cases had in mind. With trial fast approaching, and apparently facing a very real possibility that the clock would run out before the prosecution could collect the important evidence saved in d'Estree's cell phone, Agent Fink took a shortcut and made a conscious decision to open the phone using the PIN code that she knew full well had been

---

[3] Notably, several states have rejected the reasoning of *Nix* altogether and held as a matter of state constitutional law that the prosecution must demonstrate the absence of bad faith for the inevitable discovery rule to apply. *See Garnett v. State*, 308 A.3d 625, 648 (Del. 2023) ("[O]ur holding that the inevitable-discovery exception is compatible with Article I, § 6 [of the Delaware Constitution] assumes that it will be applied only when it is clear that 'the police have not acted in bad faith to accelerate the discovery of the evidence in question.'") (citation omitted); *State v. Holly*, 2013 ND 94, ¶ 55, 833 N.W.2d 15, 33 ("When a shortcut is taken that circumvents the requirements of the Fourth Amendment, the requirements of the inevitable-discovery doctrine have not been met."); *Smith v. State*, 948 P.2d 473, 481 (Alaska 1997) (recognizing the inevitable discovery rule but limiting its application under the Alaska Constitution "where the police have intentionally or knowingly violated a suspect's rights"); *Commonwealth v. Sbordone*, 678 N.E.2d 1184, 1190 (Mass. 1997) (The inevitable discovery rule may apply "as long as the officers did not act in bad faith to accelerate the discovery of evidence, and the particular constitutional violation is not so severe as to require suppression.").

illegally obtained. If ever there was a time that called for an adverse consequence, this was it. Otherwise, we would be sanctioning precisely the type of unlawful police conduct that the exclusionary rule was intended to discourage.