Case No. S068894

IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON, Plaintiff–Respondent, *Petitioner on Review*, v. AHMED GBANABOM TURAY, Defendant–Appellant, *Respondent on Review*.	Washington County Circuit Court Case No. 17CR59493 Court of Appeals Case No. A166973 Supreme Court Case No. S068894

BRIEF OF AMICI CURIAE THE AMERICAN CIVIL LIBERTIES UNION AND THE AMERICAN CIVIL LIBERTIES UNION OF OREGON IN SUPPORT OF DEFENDANT–APPELLANT TURAY

Review of the Decision of the Court of Appeal from a Judgment
of the Circuit Court for Washington County
Hon. OSCAR GARCIA, Judge

Kelly K. Simon, OSB#154213
Rachel Dallal, TPN# T22032103
(temporarily licensed in Oregon, barred in Washington)
AMERICAN CIVIL LIBERTIES UNION OF OREGON
P.O. BOX 40585
Portland, OR 97240
Telephone: (503) 444-7015
E-mail: ksimon@aclu-or.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 343-0758
E-mail: jgranick@aclu.org

* *Pro hac vice application forthcoming*

Counsel for Amici Curiae The American Civil Liberties Union & American Civil Liberties Union of Oregon

Additional counsel listed on following page.

March 2022

Ellen F. Rosenblum, OSB#753239
Attorney General
Benjamin Gutman, OSB#160599
Solicitor General
Peenesh Shah, OSB#112131
Assistant Attorney General
1162 Court Street NE
Salem, OR 97301-4096
Telephone: (503) 378-4402
E-mail: peenesh.h.shah@doj.state.or.us

Attorneys for Petitioner on Review

Ernest Lannet, OSB#013248
Chief Defender
Eric R. Johansen, OSB#822919
Deputy Public Defender
Office of Public Defense Services
1175 Court Street NE
Salem, OR 97301
Telephone: (503) 378-3349
E-mail: eric.r.johansen@opds.state.or.us

Attorneys for Respondent on Review

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Constitutional Provisions

INTERESTS OF AMICI CURIAE

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The American Civil Liberties Union of Oregon ("ACLU of Oregon") is the Oregon state affiliate of the national ACLU.

Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and as amicus in *State v. Pittman*, 367 Or. 498, 479 P.3d 1028 (2021) (en banc), *People v. Hughes*, 506 Mich. 512, 958 N.W.2d 98 (2020), *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The ACLU of Oregon has appeared frequently before this Court and federal courts advocating for the right to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article I, section 9 of the Oregon Constitution, including in *Pittman*, 367 Or. 498, 479 P.3d 1028, *United*

States v. Mohamud, 843 F.3d 420 (9th Cir. 2016), and *United States v. Pineda-Moreno*, 688 F.3d 1087 (9th Cir. 2012).

FACTUAL BACKGROUND

Detectives in Beaverton were investigating advertisements listed on the website Backpage offering sex with a minor, J, individually or with an adult woman named Gregg. Police arranged a "date" with J, who was dropped off by an unknown man. J eventually identified Turay, the defendant in this case, as the person who dropped her off. Officers located and stopped Turay in his car, seizing several cell phones, a pack of condoms, and a motel room key from the vehicle. They then sought and obtained a warrant to search the contents of the seized phones. The warrant specified nine categories of information to be "searched, seized, and analyzed":

1. Any and all communications (voice, email, text, or otherwise) between [J, Gregg, and/or defendant].

2. Evidence related to the relationship between [J, Gregg, and/or defendant].

3. Evidence regarding any communications (voice, email, text, or otherwise) involving prostitution related activities.

4. Any photos of [J, defendant, or Gregg] that show an association with prostitution including any profiting from prostitution.

5. Images, videos and/or data which depict [J or Gregg] in sexually explicit positions or conduct that relate to internet postings or advertisements.

6. Any evidence related to use of internet sites associated with prostitution, including backpage.com for a period of time 06/15/2017 to 09/06/2017.

7. Any evidence related to the use of Uber or other ride-sharing or taxicab companies.

8. Any evidence regarding the locations, including geolocation information, of the phones for a period of time from 06/15/2017 to 09/06/2017.

9. Any other evidence related to the crimes of Prostitution (ORS 167.007), Promoting Prostitution (ORS 167.012) and/or Compelling Prostitution (ORS 167.017).

See ER at 3–4.

Turay moved to suppress all information obtained as a result of these searches, arguing that the affidavit filed in support of the warrant application failed to establish probable cause or, in the alternative, was insufficiently particular and was overbroad under Article I, section 9. The trial court denied the motion and admitted the evidence. Turay was convicted of one count of compelling prostitution, ORS 167.017. *State v. Turay*, 313 Or. App. 45, 493 P.3d 1058 (2021), *rev. allowed*, 369 Or. 69 (Dec. 9, 2021).

The appellate court rejected Turay's probable cause claim. With respect to the particularity and overbreadth claims, however, the court applied *State v. Mansor*, 363 Or. 185, 421 P.3d 323 (2018), this Court's landmark case holding, in part, that a warrant authorizing a search of digital data must specify both *what* information is sought and—to the extent

possible—*when* that information was created (*e.g.*, by providing date ranges to narrow the search). Under the *Mansor* framework, the appellate court concluded that:

> **The first two search commands lacked particularity because they included no restrictions as to the time or subject matter of the information sought** and could therefore be read to authorize a "general search" for "anything incriminating."
>
> The **seventh and ninth search commands lacked particularity**, since J's mention of ride-sharing app was part of a conceded lie to protect the defendant, and because neither command included date or location limitations despite the availability of such limiting information to law enforcement.
>
> **The eighth command—for *all* geolocation data over a three-month period—**likewise **lacked the requisite specificity** because it did not include descriptions of locations or activities that would reasonably limit what police could seek. (The court described this provision as "amount[ing] to a general hunt through the phone for its whereabouts for three months . . . ." *Turay*, 313 Or. App. at 59).
>
> Finally, while a closer case, the court held that the **fourth command was defective** for its use of the vague phrase "association with prostitution" to narrow the type of information police could seek. Because the rest of the affidavit did not provide any saving context that would narrow this phrase to only that information supported by probable cause, the court held that the fourth search command was also insufficiently particular.
>
> The court held that only the third, fifth, and sixth commands were sufficiently particular.

The appellate court next addressed the question of what a court should do when it concludes that some, but not all, of a digital data warrant is insufficiently particular. The court rejected the State's suggestion that any data that *could* have resulted from a lawful section of the warrant should stand, emphasizing that Article I, section 9 rights hinge on how the search was actually conducted—not how it *might* have been conducted. *Turay*, 313 Or. App. at 65. Therefore, it held, courts in these situations must hold a hearing wherein the State must establish that the evidence sought to be utilized was actually discovered through a search or forensic analysis responsive to the surviving, constitutional portion of the warrant. *Id.* at 66. The court then remanded for the district court to make this factual finding. *Id.*

This Court granted review. *Turay*, 369 Or. 69. The State has conceded in its brief on the merits that the second, seventh, and ninth search commands were invalid. *See* Pet'r Br. at 13, 22–23, 28–29, 32. That leaves the first, fourth, and eighth commands in dispute before this Court.

INTRODUCTION AND SUMMARY OF ARGUMENT

This Court has recognized that cell phones today generate and store a huge amount of extremely revealing information about the people who use them. *Mansor*, 363 Or. at 209–10 (citing the "unique characteristics of the

cell phone described in *Riley* [*v. California*, 573 U.S. 373 (2014)]"). Warrants for cell-phone searches must closely adhere to the probable cause showing, lest authority to search a device for evidence of one crime mutate into authority to search the entirety of the device for evidence of any crime—a prohibited general search. In *Mansor*, this Court held that warrants meet the probable cause obligation by describing what *information* related to the alleged criminal conduct may be found on the device, as well as by imposing a *temporal limitation* on the search, if one is available and relevant. 363 Or. at 216–17. The Court also held that, because even a narrowly drawn search term will mean that law enforcement examines some information that is not responsive to probable cause, Article I, section 9 does not allow the State to use that information. *Id.* at 221.

These are critical provisions for ensuring that searches of extensive and sensitive personal data do not overstep constitutional bounds. But here, the State seeks to roll back *Mansor*'s protections by advocating for broad and imprecise rules that will not effectively guide issuing courts. Pet'r Br. at 2–3. The Court should reject the State's proposed rules of law, which neither provide adequate guidance to courts nor ensure that warrants issued in accordance with the proposed rules will be constitutional. Warrants must not permit rummaging searches through any data on a device, an outcome that

the State's proposed rules would allow. The State's proposals muddle rather than improve on the rule this Court cites in *Mansor*: A "warrant must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used." 363 Or. at 218.

Further, in *Mansor*, the Court did not address the conditions under which warrants must identify the *type* of computer file to be sought,[1] although it suggested that such a requirement would be "unworkable." *Id.* at 215. Amici request that the Court consider the question in this case, and hold that warrants usually can and—where possible—*should* limit police searches by relevant file type.

It is true that an issuing judge can only "describe what investigating officers believe will be found on electronic devices with as much specificity as possible under the circumstances." *Id*. at 216 (quoting *Wheeler v. State*, 135 A.3d 282, 304 (Del. 2016)). And in some cases, courts may not be able to describe a specific *file or type* of digital evidence supported by probable

---

[1] The defendant in *Mansor* did not make this argument before this Court. 363 Or. at 341 ("Defendant clarifies that that element [of what investigating officers believe will be found on the electronic devices] does not necessarily mean the type of computer file, such as an email, text, or photograph.")

cause. However, that will not usually be the case. Indeed, courts often will have sufficient context to limit search warrants to types of computer files, such as images, text messages, word-processing documents authored by the computer owner, or similar. These categories can be further refined by keyword searches, restricting police access to chats only between suspects, for example.

The rules amici propose do not limit *where* on a device law enforcement may search for relevant information,[2] but they do do ensure that a search is narrowly tailored to capture only the *type* of data supported by probable cause, wherever it may be stored. For instance, modern forensic tools are designed to identify relevant data even if it is housed in unexpected places throughout the hard drive, whether innocently or due to an intentional effort to conceal its whereabouts. Deployment of these forensic capabilities reduces or eliminates the need to search digital files indiscriminately in order to uncover hidden evidence. Forensic tools also enable effective judicial oversight, as courts can require forensic analysts to keep a query log demonstrating their search procedures, thereby allowing judges to verify that

[2] In *Mansor*, this Court rejected the defendant's argument that warrants must identify places or specific locations where evidence is likely to be found on the computer. 363 Or. at 216–17.

evidence was not acquired through inappropriate rummaging.

Additionally, where the data targeted by a digital search is stored by an Internet communication service, such as a social media platform, an effective warrant can even more easily specify the type of data relevant to the inquiry. This is because third-party platforms house and organize data independently of their users, meaning that a criminal suspect *cannot* disguise one type of data (such as device location history) as another (such as tagged photos) on, for instance, a Facebook account in the same way that is theoretically possible, at least for a sophisticated user, on a hard drive. Therefore, if it is clear in a given case that communications between two social media accounts are likely to be relevant, it is probably unnecessary for a search warrant to authorize seizure of all those accounts' posted videos, for which there is no probable cause, as well.

It is worth noting that the three search commands the appellate court held were valid already tend to define permissible searches by something like file type. Command (3) permits a search for communications and specifies that this means voice, email, text, or other forms of communication. Command (5) identifies the permissible types of files to search as images, videos, or "data which depict[s]" J or Gregg engaged in conduct related to the charges. Command (6) permits a search of any

evidence related to use of internet sites associated with prostitution, specifically backpage.com. This could be rephrased as permitting a search of relevant "internet search and/or browser history."

Finally, when searches happen pursuant to invalid warrant provisions, as apparently happened here, the evidence from those searches must be suppressed, even if the information *could* have been searched for and discovered under a valid provision.

ARGUMENT

I. THE STATE'S PROPOSED RULES OF LAW VIOLATE THE FEDERAL AND STATE CONSTITUTIONS.

The State argues for two rules of law regarding particularity requirements for warrants for electronic searches. First, the State proposes that a warrant's search command is sufficiently particular if it provides a "reasonable degree of certainty [as to] whether a particular piece of data falls within the scope of that search command, **no matter how broad that scope is**." Pet'r Br. at 2–3 (emphasis added). Second, the State proposes that a search command is not overbroad so long as it is "within the scope of the probable cause supporting it. . . . Even if that description **is not certain or precise enough to meet the specificity standard**." *Id.* at 3 (emphasis added). Alone or together, these rules do not adequately guide judges issuing

warrants and are insufficiently protective of privacy in electronic information stored on a cell phone or hard drive.

The State's proposed rules of law would lead judges in Oregon to issue unconstitutional warrants. Assume that police presented an affidavit establishing probable cause to believe that the defendant took photographs on his cell phone of paraphernalia associated with selling illegal drugs on June 12. The corresponding warrant would authorize a search of "all data stored on the defendant's phone for photos related to drug sales on June 12." That warrant would satisfy the *temporal* limitation requirement of *Mansor*. But it is not particular and would allow extensive rummaging through *all* data on the phone. Yet, under the State's proposed rules, the government could argue that the warrant is sufficiently particular because it identifies the information sought—photos related to drug sales on June 12. As such, the warrant arguably specifies the data subject to search—even though, in this case, that means *all* data from a particular date. Further, the State's proposed rules would treat this warrant as not overbroad, because the police would know to a "reasonable degree of certainty" that the drug paraphernalia photos must fall within the specified category of information to search—because that category includes *everything* on the phone.

But this is not what either the state or federal constitution allows. Valid warrants must, to the extent possible, limit the personal data accessed and reviewed by investigators to specifically that for which there is probable cause.[3] There will rarely, if ever, be probable cause to believe that *all data* stored on a given device, even with a date limitation, will relate to whatever crime is under investigation. The State's malleable proposed rules, however, would permit warrants to authorize these sweeping searches.

The Court should reject the State's arguments. As the logic of *Mansor*—and that of other privacy-protective opinions from courts around the country—demonstrates, warrants for digital data should to the extent possible describe the data sought, the relevant time frame, and the types or categories of files likely to contain the desired evidence. And as the facts of *Mansor* show, warrants *can* effectively limit searches by category of data, such as Internet search history, without leaving police investigations at the mercy of the changeable nature of electronic data. Modern forensic techniques and the practical logistics of digital searches enable and require that police narrow their focus in searching cell phones and other computers. The warrant can and must guide that search to be constitutional.

---

[3] It is not clear whether the State's "reasonable degree of certainty" is more, less, or the same as probable cause, which the Constitution requires.

II. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA.

Smartphones are ubiquitous, highly portable devices that "place vast quantities of personal information literally in the hands of individuals." *Riley*, 573 U.S. at 386. Americans use their phones for a wide variety of purposes and, as a result, smartphones contain a voluminous and varied collection of data. While data is often organized by application or file type, even discrete categories of information—alone or in combination with each other—comprise a "digital record of nearly every aspect of [our] lives." *Id.* at 375.

Cell phone use is now deeply entrenched in the fabric of daily life. Ninety-seven percent of Americans own a cell phone and 85% own a smartphone specifically.[4] These devices are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of the human anatomy."*Riley*, 573 U.S. at 385. Mobile devices have become the screen that people access first and most often.[5] Nearly half of Americans check their smartphones as soon as

---

[4] Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021), https://www.pewinternet.org/fact-sheet/mobile/.

[5] John Koetsier, *We've Spent 1.6 Trillion Hours on Mobile So Far in 2020*, Forbes (Aug. 17, 2020),

they wake up in the morning.[6] People proceed to spend an average of four hours a day using various apps on their phones.[7] Cell phone use is so persistent that the medical field has adopted a term to describe the intense anxiety many people experience when they fear being separated from their cell phones: *NOMOPHOBIA: NO MObile PHone PhoBIA*.[8]

Americans' dependency on smartphones has, intentionally and inadvertently, resulted in our phones containing vast troves of our personal information. Indeed, cell phones "differ in both a quantitative and a qualitative sense" from other objects because of "all [the personal information] they contain and all they may reveal." *Riley*, 573 U.S. at 393, 403. The "immense storage capacity" of smartphones allows them to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and to store

---

https://www.forbes.com/sites/johnkoetsier/2020/08/17/weve-spent-16-trillion-hours-on-mobile-so-far-in-2020/.

[6] Diane Thieke, *Smartphone Statistics: For Most Users, It's 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017), https://www.reportlinker.com/insight/smartphone-connection.html.

[7] App Annie, *The State of Mobile 2021* 7 (2021), available at https://www.appannie.com/en/go/state-of-mobile-2021/.

[8] Sudip Bhattacharya et al., *NOMOPHOBIA: NO Mobile Phone PhoBIA*, 8 J. Fam. Med. Prim. Care 1297 (2019), available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6510111/.

extensive historical information related to each functionality. *Id.* at 393. Because a cell phone "collects in one place many distinct types of information"—for example, an address, a note, a prescription, a bank statement, or a video— cell-phone data "reveal much more in combination than any isolated record," *id.* at 394, and they reveal much more about "an individual's private interests or concerns." *Id.* at 395.

The broad range of applications available to cell phone users and the ever-increasing amount of storage on new-generation devices mean that digital searches today implicate more data than ever before. For instance, one in five Americans currently use health-related smartphone apps—sometimes linked to wearable devices—to track information related to their location, movement and sleep patterns, heart rate, nutrition, menstrual cycles, and other sensitive health data.[9] Other apps may monitor home security cameras, facilitate dating (and thereby reveal the user's sexual

---

[9] Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, Gallup (Dec. 11, 2019), https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx; Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020), https://www.lifewire.com/what-wearables-can-track-4121040/; Geoffrey A. Fowler & Heather Kelly, *Amazon's New Health Band Is the Most Invasive Tech We've Ever Tested*, Wash. Post (Dec. 10, 2020), https://www.washingtonpost.com/technology/2020/12/10/amazon-halo-band-review/.

orientation), track a household's budget, manage financial accounts, or send encrypted messages.[10] Coupled with devices' rapidly increasing storage capacities, these apps mean that any given person's cell phone may reveal a comprehensive portrait of their health, their location history, their sexual preferences, their private conversations, their photos, their finances, their social and professional networks, and a myriad of other things from taste in music to political beliefs. In short, cell phones produce "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." *Riley*, 573 U.S. at 395. While a single app or type of data can reveal an extraordinary amount about a person, the combination of the many different types of data on a phone can essentially reconstruct a person's life.

---

[10] *See, e.g.*, Blink, *Blink Home Monitor App*, https://blinkforhome.com/blink-app (last visited Mar. 29, 2022); Grindr, *About Grindr*, https://www.grindr.com/about/ (last visited Mar. 29, 2022); Kinkoo, *Kinkoo*, https://www.kinkoo.app/ (last visited Mar. 29, 2022); Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, Forbes (Feb. 24, 2021), https://www.forbes.com/advisor/banking/digital-banking-survey-mobile-app-valuable-features/; Mary Meeker, *Internet Trends 2019*, Bond Capital, at 168 (June 11, 2019), available at https://www.bondcap.com/report/itr19/; Jack Nicas, Mike Isaac, & Shira Frenkel, *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, N.Y. Times (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.

Therefore, as this Court has recognized, Article I, section 9, "must be read in light of the ever-expanding capacity of individuals and the government to gather information by technological means." *Mansor*, 363 Or. at 373.

III. WARRANTS CAN LIMIT LAW ENFORCEMENT SEARCHES BY CATEGORY OF DATA.

A. *Mansor* recognizes that warrants must be particular and not overbroad, especially when authorizing searches of digital devices.

The text and principles of Article I, section 9, can be traced directly to the Fourth Amendment to the United States Constitution. Under both provisions of law, it is axiomatic that officers must have probable cause to support the search of a cell phone. *See generally Mansor*, 363 Or. 185; *Riley*, 573 U.S. 373. Further, probable cause to search or seize *some* data on the phone cannot justify access to the totality of the phone's contents; instead, warrants must offer sufficiently particular instructions and avoid giving law enforcement license to search an overly broad swath of information. Given the vast amounts of personal data stored on phones, and all that can be gleaned from that data, strict limits on digital searches and seizures are crucial to preserve privacy. *See, e.g.*, *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (discussing the need for "heightened sensitivity to the particularity requirement in the context of digital searches" due to the vast

amount of information that digital devices contain); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam), *overruled in part on other grounds by Demaree v. Pederson*, 887 F.3d 870 (9th Cir. 2018) (discussing the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant"); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store "a huge array" of information "makes the particularity requirement that much more important").

In *Mansor*, this Court held that "warrant[s] must identify, as specifically as reasonably possible in the circumstances, the information to be searched for, including, if relevant and available, the time period during which that information was created, accessed, or otherwise used." 363 Or. at 187–88. Further, *Mansor* held that warrants must describe, to the greatest degree of specificity possible, the information that law enforcement is authorized to search and seize—in other words, the data for which there exists probable cause. As this Court has emphasized, law enforcement may not "rummag[e]" indiscriminately through the vast amount of sensitive information stored on cell phones. *Id.* at 220.

The question remains, however, whether warrants should limit digital

searches by *file type* (for instance, authorizing the search and seizure of text messages, but not photos, from a specific time period). The *Mansor* Court did not reach this issue because the defendant did not pursue it. Thus, while the Court rejected the contention that warrants for digital devices should limit *where* investigators may search, such as a "My Documents" or "Downloads" folder, *id.* at 216, the Court did not consider whether they should require a list of relevant file *categories*. *Id*. ("Defendant clarifies that that element [of what investigating officers believe will be found on the electronic devices] does not necessarily mean the type of computer file, such as an email, text, or photograph."). However, this Court suggested that it agreed with the court in *Wheeler*, 135 A.3d at 305, that limitations on types of files officers could search would be "unworkable." *Mansor*, 363 at 215.

This is the question *amici* ask the court to address in this case.

B. Use restrictions, while essential, are not enough on their own to shield private and sensitive digital data.

Use restrictions on non-responsive data obtained pursuant to a lawful warrant are an essential Fourth Amendment protection for the reasons this Court stated in *Mansor*. The intermingled nature of digital data means that "[e]ven a reasonable search authorized by a valid warrant necessarily may require examination of at least some information that is beyond the scope of the warrant." *Id.* at 220. As this Court recognized, this means that there is

always a risk that search warrants for digital devices could inadvertently become the electronic equivalent of general warrants, sanctioning the "undue rummaging that the particularity requirement was enacted to preclude." *Id.* (internal quotation marks omitted). Thus, even where warrants authorize, and officers conduct, only reasonable searches, "individual privacy interests preclude the state from benefiting from that necessity by being permitted to use that evidence at trial." *Id.* at 220–21. The State may not use information obtained in a computer search if the warrant did not authorize the search for that information, unless some other warrant exception applies. *Id.* at 221 (citing Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 24 (2015) (advocating for use restrictions for data "nonresponsive" to the warrant)).

This rule instantiating use restrictions is privacy protective and disincentivizes police overreach—law enforcement would be disinclined to search too broadly if courts will exclude nonresponsive or inappropriately obtained evidence. However, use restrictions do not fully protect a person's privacy and are at best an incomplete remedy. When a law enforcement cellphone search exceeds the scope of probable cause, investigators learn intimate information about the individual's life, *regardless* of whether that

data is ultimately excluded at trial. Further, if an overbroad search leads to useful information, investigators will be incentivized to use "parallel construction," an opaque and controversial (if not always illegal) technique whereby the government manufactures an alternative, valid discovery route for evidence obtained through illegal means or via techniques the government would rather not have publicly known or reviewed by a court. *See* Hum. Rights Watch, *Dark Side: Secret Origins of Evidence in U.S. Criminal Cases* (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013), https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805 (parallel construction used to protect the DEA's use of information from intelligence intercepts, wiretaps, and a massive database of telephone records); Jenna McLaughlin, *FBI Told Cops to Recreate Evidence from Secret Cell-Phone Trackers*, The Intercept (May 2016), https://theintercept.com/2016/05/05/fbi-told-cops-to-recreate-evidence-from-secret-cell-phone-trackers/; Jessica Glenza & Nicky Woolf, *StingRay Spying: FBI's Secret Deal with Police Hides Phone Dragnet From*

Courts, The Guardian (Apr. 10, 2015), https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-dragnet-police; Jennifer Granick, *American Spies* 178, 224 (2017).

There is also the danger that, with enough information, police could concoct a story to support their prosecution of the original crime, even if the evidence for such a crime was sparse at the time the warrant was issued. "If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him." Armand Jean du Plessis, Cardinal-Duc de Richelieu et de Fronsac as cited in Jehiel Keeler Hoyt, *The Cyclopedia of Practical Quotations* 763 (1896).

Finally, use restrictions do not protect an individual's privacy in any instance where that person is not ultimately charged with a crime.

In sum, use restrictions—while a critical tool to ensure that illegally obtained information is not used to convict a defendant—are insufficient to protect the full extent of the substantial privacy interests at stake in digital searches.

C. A general requirement that warrants identify relevant file types is reasonable and effective for law enforcement.

Warrants can limit searches for electronic evidence by file type as well as by description and time without unduly interfering with law enforcement investigations. If there is probable cause to believe that co-

conspirators texted each other, there is no reason in the first instance to search photos. If investigators learn that suspicious texts attach photos, then the search can expand to those (and related) photos, either pursuant to a second warrant, or under the first warrant, as overseen by the issuing judge. This is not a heavy lift.

Widely used forensic software is capable of limiting searches to particular categories of data, which can then be sub-searched for the information approved in the warrant. As with e-discovery tools, such forensic software can also generate query or audit logs that supervising officers, prosecutors, magistrates, and defense attorneys can review to ensure that searches were performed in a narrow and constitutional manner.

There is U.S. Supreme Court precedent to support limiting searches by file type or category. *Riley* explicitly discussed the invasiveness of law enforcement access to different "categories," "areas," "types" of data, and "apps." 573 U.S. at 395, 396, 399. The Court also pointed out that "certain types of data are also qualitatively different" from others in terms of privacy. *Id*. at 395. As the Fifth Circuit recently put it, the lesson of *Riley* is that "distinct types of information, often stored in different components of the phone, should be analyzed separately." *United States v. Morton*, 984 F.3d

421, 425 (5th Cir. 2021), *reh'g en banc granted*, 996 F.3d 754 (5th Cir. May 18, 2021).

With increasing frequency, courts have followed *Riley* to hold that looking at the right categories of data, not all data, is the only plan that makes sense and complies with the Constitution. *See, e.g.*, *State v. Bock*, 310 Or. App. 329, 335, 485 P.3d 931 (2021) (warrants may not authorize searches through any and all contents of electronic files that may contain circumstantial evidence about the owner or evidence of identified criminal offenses); *Burns v. United States*, 235 A.3d 758, 775 (D.C. Cir. 2020) (warrant authorizing search for categories of data for which there was no probable cause was "constitutionally intolerable"); *People v. Musha*, 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) (in child abuse case, there was probable cause to search the phone's photographs, but not to examine web search history); *State v. McLawhorn*, 636 S.W.3d 210, 239–44 (Tenn. Crim. App. 2020) (officers cannot search entirety of phone to determine whether device has flashlight function); *Taylor v. State*, 260 A.3d 602 (Del. 2021) (warrant permitting search and seizure of "any/all data stored by whatever means" failed the Fourth Amendment and state constitutions' particularity requirements); *In re United States of America's Application for a Search Warrant to Seize and Search Elec. Devices from Edward Cunnius*, 770 F.

Supp. 2d 1138, 1147–1151 (W.D. Wash. 2011) (application to search and seize "all electronically stored information . . . contained in any digital devices seized from [defendant's] residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods" was improper because it sought "the broadest warrant possible," and did not propose to use a search technique that foreclosed the plain view doctrine's application to digital materials). As these cases demonstrate, even when there is probable cause to search a device for *something*, courts routinely hold that file types that are not connected to the probable cause showing may not be accessed or examined.

To be clear, warrants should limit searches based on time frame, information sought, *and* file type—especially when authorizing searches of sensitive categories of data such as personal conversations. For example, in *People v. Herrera*, 357 P.3d 1227 (Colo. 2015), the Colorado Supreme Court suppressed evidence contained in a text message involving a third party not named in the warrant. The court held that the government's argument that *any* text message folder could be searched because of the abstract possibility that the folder might contain indicia of who owned the phone, or might have been deceptively labeled, would result in an unconstitutional limitless search. *Id.* at 1230, 1233–34. Thus, the appropriate

search criteria would have identified the relevant file type (text messages) *and* the text conversations relevant to the inquiry (those involving the individuals named in the warrant). These functional limitations can be constitutionally required, as the law is clear that police cannot get a warrant to seize or search categories of data for which there is no probable cause. *See, e.g.*, *In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014).

D. Under careful judicial supervision, forensic tools enable highly effective and properly scoped searches and seizures of digital material.

Search features, as well as forensic tools, can narrow down the information an investigator seeks to only that which is responsive to key terms—just as one might use Google to search the web—and can display information about the results and their location on the device. Investigators can refine their queries using keyword searches, including Boolean queries like those lawyers use in a Westlaw search. Moreover, the power of these tools makes it far more difficult, perhaps impossible, for the casual computer user to effectively hide, obscure, or mislabel evidence.

The tools also perform targeted searches, which enable investigators to comprehensively and efficiently home in on the digital evidence most likely to be warrant-responsive, while ignoring other information.

Investigators can limit a search to a particular date range, allowing analysts to obtain files within temporal proximity of the relevant crime.[11] Forensic tools can also search based on file category or type. For example, EnCase Forensic Software ("EnCase") is a law enforcement search tool for hard drives and mobile devices. EnCase can be configured to search for specific files or types of data on a computer—such as emails, Internet searches,[12] photographs,[13] documents,[14] files over a specified size,[15] files with a particular extension,[16] files containing personal identifying information (such as email addresses and credit card, Social Security, and phone numbers),[17] or files containing certain keywords.[18] Law enforcement widely

---

[11] *See, e.g.*, AccessData, *Forensic Toolkit User Guide* 102 (2017), available at https://ad-pdf.s3.amazonaws.com/ftk/FTK%206.1/FTK_UG.pdf (FTK User Guide) ("Refine evidence further by making the addition of evidence items dependent on a date range or file size that you specify. However, once in the case, filters can also be applied to accomplish this.").

[12] Guidance Software, *EnCase Forensic User Guide Version 8.07* 64–65 (2018), available at http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf.

[13] *Id.* at 62.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.* at 338.

[18] *Id.* at 143, 246.

uses these forensic tools because they search regardless of how the information is stored or named. For example, while file extension search filters are imperfect (since a suspect could disguise a photo by resaving a ".jpg" to a ".doc" extension),[19] "file header" functionalities on EnCase can determine a file's format regardless of filename or extension.[20] Forensic software programs can also detect embedded file images—that is, photographs hidden inside of Microsoft Word documents.[21] And while keyword searches can be imperfect,[22] today Optical Character Recognition ("OCR")—a common forensic tool which automatically extracts text contained in graphic files, such as images or non-searchable PDFs—

---

[19] Computer Crime & Intellectual Prop. Sect., Crim. Div., U.S. Dep't of Just., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 36 (2009), available at https://perma.cc/VP23-RZTJ (DOJ Manual) (quoting *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006)).

[20] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 545 (2005).

[21] *See, e.g.*, AccessData, Forensic Toolkit User Guide 139 (2017), https://ad-pdf.s3.amazonaws.com/ftk/FTK%206.1/FTK_UG.pdf (FTK User Guide) ("To recover embedded or deleted files, the case evidence is searched for specific file headers. . . . Embedded or deleted items can be found as long as the file header still exists.").

[22] DOJ Manual at 79.

addresses that challenge.[23] EnCase can also automatically identify illegal files (such as child pornography) without a human investigator needing to open the file.

Forensic tools may also have a search history feature, just as eDiscovery tools do.[24] Such query or audit logs facilitate a post-search review to ensure law enforcement complied with the dictates of the warrant. With such logs, judges could better understand the precise steps that law enforcement took when search a cell phone. In particular, these logs could equip judges to better assess the reasonableness of the search technique and ascertain if the search was sufficiently narrowly tailored to the warrant. If courts were to insist upon the production of digital audit logs created by the forensic tool upon the return of a search warrant, tool vendors that do not already provide this functionality would rapidly develop this feature.

---

[23] FTK User Guide at 95 ("The [OCR] process lets you extract text that is contained in graphics files. The text is then indexed so that it can be[] searched[] and bookmarked.").

[24] *See, e.g.*, Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft Docs (Jan. 7, 2022), https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide (Content search and eDiscovery-related activities are logged in the audit log when creating, starting, and editing Content searches, and performing search actions, such as previewing, exporting, and deleting search results, among other activities.).

There are many such products on the market and available to law enforcement at the state and local level, as well as to the FBI. For instance, similar tools include Forensic ToolKit and Cellebrite. Research by the firm Upturn shows that mobile device forensic tools are widely available even to smaller law enforcement agencies, which either purchase them outright, obtain them through federal grants, or work with larger local law enforcement agencies that conduct extractions of data at the smaller agencies' request. Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020), available at https://perma.cc/7DCK-PGMQ.

In sum, forensic search tools can therefore make searches limited by file type workable, while also being effective for law enforcement. Certainly, limiting searches by file category or type will not always be possible. But it often is, and in those situations, this Court should require that warrants indicate, and officers observe, that limitation.

File-type limitations are not, however, a panacea—and they require judicial regulation to be used both effectively and lawfully. Like any search technique, forensic search tools can be over- or under-inclusive. And forensic tools can extract more and different types of data than manual searches, and analyze that data far more efficiently than human reviewers

acting alone. Indeed, they can even reveal information that the owner does not know is there, and, by gathering hidden and deleted files, exacerbate the potential for indiscriminate and overbroad searches. As with manual searches, forensic searches potentially expose substantial amounts of irrelevant info to manual review by investigators. For this reason, some technical experts have warned that forensic search tools "are simply too powerful in the hands of law enforcement and should not be used."[25]

However, proper warrants and judicial oversight can ensure that these powerful tools are used in ways that reduce rummaging, limit law enforcement agents' exposure to non-responsive information, and enable judicial oversight and auditing of the search process.

E. Warrants can effectively limit by data category government searches and seizures of social media account information.

Seizures and searches of information stored in social media or other online accounts are different from those seeking data stored on a phone or hard drive. In the latter case, officers will typically seize computer hardware,

---

[25] Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* 5. The Upturn report recommends at a minimum banning consent searches of mobile devices, abolishing the plain view exception for digital searches, and requiring easy-to-understand audit logs, enacting robust data deletion and sealing requirements, and requireing clear public logging of law enforcement use.

which contains all data on a device, and then extract that data for forensic analysis. The vast majority of the extracted data is irrelevant to the case, and highly intimate. This is why having a warrant effectively narrow the search is so important.

In contrast, obtaining every bit of information in an online account will usually be unnecessary, because it is relatively simple to identify, request, and seize only the categories of data relevant to the inquiry. For instance, providers preserve account data after the receipt of a warrant, so spoliation is less of a concern than when officers must seize a device from the suspect's possession. In addition to being able to preserve data, service providers have the capability of filtering out irrelevant data as directed by a warrant. Investigators can work with providers to ensure that only responsive information, as defined by the warrant, is ultimately disclosed.

Notably, it is not currently possible to hide evidence in the context of a Facebook or other social media account in the same way as a sophisticated computer user might be capable of on a hard drive or other local storage. *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017), *cert. den. sub nom*. *Blake v. United States*, 138 S. Ct. 1580 (2018). Information associated with an online account is stored, categorized, and sorted by the company—not by the user. Providers are able to effectively distinguish images from

text, find material by date, and filter conversations by participant or even keyword. Even sophisticated criminals cannot effectively hide evidence behind misleading file names or types online. "[T]here is no possibility that a user could have filed an incriminating photo as a 'poke,' and there is no chance that an incriminating message will be stored as a third-party password or a rejected friend request." *United States v. Shipp*, 392 F. Supp. 3d 300, 309 (E.D.N.Y. 2019). The platform organizes the information in such a way that even a technologically sophisticated criminal cannot effectively conceal information in a different category of information, making broad searches especially unnecessary.

Further, seizing the entirety of online account data raises cybersecurity and oversight concerns as well as privacy considerations. Many of the information demands that we have seen officials list as part of common boilerplate warrants should almost never be permitted, such as passwords and PIN codes. This sensitive information can be used to prospectively spy on account holders, a technique that likely requires a wiretap warrant, not a Rule 41 warrant (or its state-law equivalent).[26] It risks

---

[26] The Fourth Amendment requires safeguards beyond traditional search warrants where surveillance consists of "a series [of intrusions] or a continuous surveillance" and not "one limited intrusion." *Berger v. New York*, 388 U.S. 41, 57 (1967); *See also* Orin S. Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It*, 72

abuse by enabling officers to repeatedly access accounts without judicial oversight. Passwords can also be misused to send fake messages, impersonate the account holder, or even create false evidence—and it is a rare scenario where the password itself will constitute relevant evidence supported by probable cause.

In *Shipp*, 392 F. Supp. 3d 300, for example, a search warrant to Facebook demanded all of the suspect's personal information, activity logs, photos and videos, as well as materials posted by others that tagged the suspect, all postings, private messages, and chats, all friend requests, groups and applications activity, all private messages and video call history, check-ins, IP logs, "likes," searches, use of Facebook Marketplace, payment information, privacy settings, blocked users, and tech-support requests. *Id.* at 303–06. This list was not limited to the types of information likely to provide evidence of the specific crime under investigation. And the district court expressed "serious concerns regarding the breadth of [the] Facebook warrants." *Id*. at 307. Warrant-issuing courts "can and should take particular care to ensure that the scope of searches involving Facebook are 'defined by

---

Geo. Wash. L. Rev. 1208, 1232 (2004) (stating it is the functional equivalent of a wiretap if an agent installs software that copies incoming messages a few milliseconds after they arrive).

the object of the search and the places in which there is probable cause to believe that it may be found.'" *Id.* (citing *United States v. Ross*, 456 U.S. 798, 824 (1982)). If, for example, a case involves a conspiracy to sell drugs, the police do not need passwords, tagged posts, or "likes." In *Shipp*, the "all-content" warrant far exceeded those limits in purporting to authorize seizure of all this information.

To limit up front the information to which the government gets access, courts should reject "all-data," "all-content," or boilerplate service-provider warrants containing comprehensive lists of types of data in favor of a defined list of relevant categories of data tailored to the investigation at hand. For example, if the allegations are that a suspect sent photos of guns to prospective buyers over WhatsApp, the warrant can authorize a search of WhatsApp chats and associated photos sent through the application—passwords, location history, and other account data would be irrelevant. Keyword searches may be an option to further limit the data that a service provider discloses to law enforcement. The government must be required to narrow the data it seizes from online service providers by asking the provider to limit disclosures based on keywords, such as the name of a co-conspirator, a bank account number used for illegal proceeds, or reference to the address where a burglary took place.

For example, officers could limit the warrant to demand only messages between co-conspirators. If Bob and Alice are collaborating, Google may be able to parse just emails between those two, just as account holders can do when they search their inboxes. The government should also limit its acquisition to messages sent by the suspect, or exclude emails between suspects and their employers, identified attorneys, clergy, or spouses, or notifications from social media entities like Facebook or Twitter. *In the Matter of the Search of Premises Known as: Three Hotmail Email Accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *7, *14 (D. Kan. Mar. 28, 2016) (suggesting that warrants could direct an online service provider to produce responsive material in a manner devoid of the exercise of investigatory skill or discretion).[27] *See also In the Matter of the Search of Info. Associated with [redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145 (D.D.C. 2014), *order vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014); *In the Matter of Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*,

[27] The magistrate was overturned by the District Court, which ruled that the "seize first, search second" process did not require these limitations. *In the Matter of the Search of Info. Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016).

Nos. 13–MJ–8163–JPO, 13–MJ–8164–DJW, 13–MJ–8165–DJW, 13–MJ–8166–JPO, 13–MJ–8167–DJW, 2013 WL 4647554 (D. Kan. Aug. 27, 2013).

Images may be another area where providers' built-in search capabilities enable more tailored data seizures. For instance, Google Photos is designed to do image searches. Google, *About Google Photos*, https://www.google.com/photos/about/ (last visited Mar. 29, 2022) (explaining that photos saved to Google photos "are automatically organized and searchable" by their associated geolocation information and the things in them). Investigators might seek from Google only those photos that were taken at a particular location or that contain the image of a particular person of interest.

The main objection to having online service providers search for and disclose only a portion of online account data is that providers are poorly positioned to conduct investigations for law enforcement. Providers do not know the facts of the investigation and are not trained law enforcement actors. However, warrants with specifications such as data category limitations, time frames, email to/from limits, and photo location- or content-searches mean that providers need not understand the investigation or exercise any investigatory discretion in providing responsive information. The search terms should be clear, set by the investigators, and overseen by

the issuing magistrate or judge. Often, executing these advanced searches is well within the capability of the provider and requires no investigatory expertise. And investigators can then follow up on any leads by obtaining a second warrant.

IV. THIS COURT SHOULD HOLD THAT WHERE SOME OF THE WARRANT IS INVALID, ANY EVIDENCE ACTUALLY OBTAINED PURSUANT TO THOSE PROVISIONS SHOULD BE SUPPRESSED.

The appellate court rejected the State's suggestion that any data that *could* have resulted from a lawful section of the warrant should stand, and emphasized that Article I, section 9 rights hinge instead on how the search was *actually* conducted. This Court's jurisprudence and the principles underlying the Fourth Amendment support the appellate court's conclusion and this Court should adopt it.

"[R]ules of law designed to protect citizens against unauthorized or illegal searches or seizures of their persons, property, or private effects are to be given effect by denying the state the use of evidence secured in violation of those rules against the persons whose rights were violated." *State v. Davis*, 295 Or. 227, 237, 666 P.2d 802 (1983). One purpose of rules requiring the suppression of evidence gathered in violation of the Oregon Constitution is to restore the parties to the position they would have been in

had the violation not occurred. The exclusionary rule of section 9 is predicated on the personal right of a criminal defendant to be free from an "unreasonable search, or seizure." *Id.* at 231–37; *State v. Laundy*, 103 Or. 443, 494, 206 P. 290 (1922) (en banc).

Another goal of the suppression remedy is "to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it." *Elkins v. United States*, 364 U.S. 206, 217 (1960). "A ruling admitting evidence in a criminal trial … has the necessary effect of legitimizing the conduct which produced the evidence, while an application of the exclusionary rule withholds the constitutional imprimatur." *Terry v. Ohio*, 392 U.S. 1, 13 (1968).

Evidence is not inadmissible under Article I, section 9, simply because it was obtained after unlawful police conduct. But to save the evidence, the State must establish that the disputed evidence did not derive from the illegality. *State v. Johnson*, 335 Or. 511, 520–21, 73 P.3d 282 (2003). The test is not whether the disputed evidence *could have* be obtained lawfully, but rather whether *was* or *inevitably would have* been. *Id.* (in relevant part, state must prove that the police *inevitably* would have obtained the disputed evidence through lawful procedures even without the violation of the defendant's rights under Article I, section 9).

The State's proposed rule of law is to the contrary. It suggests that evidence obtained pursuant to invalid portions of a warrant may be admitted regardless of police conduct so long as there exists some theory under which the evidence could have fallen within the scope of a different, valid search command. This rule would not serve the purpose of the suppression remedy, which is, in part, to deter police misconduct. Police should not be applying for or executing unconstitutional searches. But the State's rule would invite them to do just that by blessing these illegal searches in at least some cases. The rule also conflicts with this Court's holding in *Johnson*, which requires that the acquisition of the evidence have been inevitable, not merely conceivable.

As in *State v. Bock*, 310 Or. App. 329, the State's argument is unworkable, and fails to serve the purpose of the exclusionary rule. Courts cannot retrace the forensic investigator's steps to determine whether a different search *might* have captured the same evidence. *Id.* at 340. Guessing what might have happened if the warrant terms were valid is a speculative enterprise beyond the scope of evidentiary proof.

Nor does such a rule provide the remedy required by Article I, section 9—making the defendant whole. As the appellate court explained, in the context of the plain view exception:

> Although it might have been "expected" that state agents would examine each photo on defendant's cell phone in searching for location data, that fact does not make the search for those photos somehow less invasive. The state still had to conduct a broad search of defendant's cell phone to find those photos to search them for location data in the first place. The breadth of the search is what renders the plain view doctrine inapplicable; the alternative would sanction the sort of general warrant that the plain view doctrine was never meant to authorize.

Id. (citing *Mansor*, 363 Or. at 220).

The court's insight is no less true here. The State's rule would bless an overbroad search pursuant to an unconstitutional warrant despite the lack of guidance to the police, and the improper review of private information.

CONCLUSION

The judgment of the Court of Appeals should be affirmed.

Dated: March 29, 2022

Respectfully Submitted,

/s/ Kelly K. Simon
Kelly K. Simon, OSB#154213
Rachel Dallal, TPN# T22032103
(temporarily licensed in Oregon,
barred in Washington)
AMERICAN CIVIL LIBERTIES
UNION OF OREGON
P.O. BOX 40585
Portland, OR 97240
Telephone: (503) 444-7015
E-mail: ksimon@aclu-or.org

Counsel continued on following page.

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 343-0758
E-mail: jgranick@aclu.org

** Pro hac vice application forthcoming*

Attorneys for Amici Curiae The American Civil Liberties Union & American Civil Liberties Union of Oregon

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that this brief complies with the word-count limitation in ORAP 5.05(1)(b)(ii)(B) because the word count on this brief (as described in ORAP 5.05(1)(d)(i)) is 8,876 words.

I certify that the size of the type in this brief is not smaller than fourteen points for both the text of the brief and footnotes, as required under ORAP 5.05(3)(b)(ii).

Dated: March 29, 2022

/s/ Kelly K. Simon
Kelly K. Simon, OSB#154213
American Civil Liberties
Union of Oregon
P.O. BOX 40585
Portland, OR 97240
Telephone: (503) 444-7015
E-mail: ksimon@aclu-or.org

Attorney for Amici Curiae The American Civil Liberties Union & American Civil Liberties Union of Oregon

CERTIFICATE OF FILING AND SERVICE

I HEREBY CERTIFY that on March 29, 2022, I caused the foregoing Brief of Amici Curiae The American Civil Liberties Union and The American Civil Liberties Union of Oregon in Support of Defendant–Appellant Turay to be electronically filed with the State Court Administrator, Records Section, by using the Court's electronic filing sytem.

I FURTHER CERTIFY that on March 29, 2022, I electronically served the foregoing Brief of Amici Curiae The American Civil Liberties Union and The American Civil Liberties Union of Oregon in Support of Defendant–Appellant Turay upon Ernest Lannet and Eric Johansen, attorneys for Appellant, and Peenesh Shah, Ellen F. Rosenblum, and Benjamin Guttman, attorneys for Petitioner, using the Court's electronic filing system.

Dated: March 29, 2022

/s/ Kelly K. Simon
Kelly K. Simon, OSB#154213
American Civil Liberties
Union of Oregon
P.O. BOX 40585
Portland, OR 97240
Telephone: (503) 444-7015
E-mail: ksimon@aclu-or.org

Attorney for Amici Curiae The American Civil Liberties Union & American Civil Liberties Union of Oregon