Preventing Overcollection of Electronic Information by Court Rule

BY LAUREN WIGGINTON, ESQ.

Probable cause for the state to charge a person with a crime does not give the State carte blanche authority to search that person's electronic devices.[1] See *United States v. Wei Seng Phua,* No. 2:14-CR-00249-APG, 2015 WL 1281603, at *7 (D. Nev. Mar. 20, 2015) (discussing warrant requirement in the electronic search context). Instead, the state must obtain a warrant, and it is then (theoretically) limited in its search to places where there is probable cause to believe an item named in the warrant could be found. *Maryland v. Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013 (1987).

This is commonly known as the "particularity requirement." *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 164–65 (D.D.C. 2014). The particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013.

The particularity requirement offers limited protection in the electronic search context.

Unfortunately, in the context of electronic searches, the effectiveness of the particularity requirement's protections is unclear. Imagine that the state obtains a warrant to search the iPhone of an individual charged with drug trafficking. The warrant identifies the phone via its International Mobile Equipment Identity number, and the evidence sought as all digitally stored records thereon that support the crime charged. Such evidence could theoretically be found anywhere in that iPhone, and could include text messages setting meeting times, places, and prices;

location data demonstrating that a phone pinged a particular cell tower at a particular time; photographs of product and/or paraphernalia; or even records of online purchases of small plastic bags and a digital scale. In effect, such a warrant gives the state authority to seize and review every digital file on the iPhone.

Once the state examines a file, it can plausibly claim that its contents are in plain view. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) ("*CDT*"). That is, if incriminating information—even as to conduct completely disparate from the crime charged—is uncovered, the state can keep and use it elsewhere. *See* James Saylor, *Computers As Castles: Preventing the Plain View Doctrine from Becoming A Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809, 2830 (2011). As the Ninth Circuit described: "Authorization to search *some* computer files therefore automatically becomes authorization to search all files in the same sub-directory, … an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media. Where computers … are connected electronically, the original search might justify examining files in computers many miles away." *Id.*

Given the scope of information held on digital devices, this is a matter of concern to individuals and businesses alike. *See* Stephen Moccia, *Bits, Bytes, and Constitutional Rights: Navigating Digital Data and the Fourth Amendment*, 46 Fordham Urb. L.J. 162, 164 (2019). A warrant—seeking, for example, all electronic data that could be evidence of a corporate director's alleged wrongful conduct—could theoretically be read to authorize the state in searching the corporation's entire remote server database. This authorization could allow the state to review the corporation's proprietary information, trade secrets, and customer personal identifying information, among a multitude of other data and documents. Even if nothing incriminating is found, the damage already caused by the external revelation of such confidential information cannot be undone.

Guidry v. State presented this question to the Nevada Supreme Court.

How to balance the need to minimize over-collection in electronic searches with the state's investigative needs is a question that is coming to the forefront in Nevada. *Guidry v. State* already teed the question up for the Nevada Supreme Court, though the court reversed Ronneka Guidry's conviction on alternative grounds. *See generally*, 138 Nev. Adv. Op. 39, 510 P.3d 782 (2022).

Eduardo Osorio fell from the hood of Guidry's vehicle, suffered a grievous head injury, and died. *Id.,* 138 Nev. Adv. Op. 39, 510 P.3d at 786. Guidry had given Osorio a ride from Caesar's Palace to the Westin, during which she somehow obtained Osorio's $8,000 Rolex. *Id.* Osorio realized that his watch was missing after exiting Guidry's vehicle. *Id.* He chased her Mercedes down, jumping onto the hood and repeatedly punching the windshield while screaming incoherently. *Id.* Osorio fell to his death as Guidry attempted to pull away. *Id.* A jury convicted Guidry of second-degree murder. *Id.*

Guidry appealed her conviction on multiple grounds, including that a search by Las Vegas Metropolitan Police (Metro) of a cell phone found in Guidry's vehicle was unconstitutional because the relevant warrant failed the particularity requirement. No. 80156 Appellant's Opening Brief ("Guidry AOB") 75-76. The warrant identified the cell phone and sought all digitally stored records thereon "which may constitute evidence of [Guidry's alleged crimes]" or "tend to establish the identity of the persons who were in … control of the [phone]." App'x to Guidry AOB, Vol. 1, p. 145. In essence, Guidry argued, the breadth of the electronic search warrant "allowed Metro to download everything on [Guidry's] phone – more than 30,000 images, call logs, location service – everything." AOB at 77.

If the court had found that search unconstitutional, it would likely have reversed Guidry's conviction and required that the evidence found thereon (which included photos of the watch and evidence that Guidry sold it on eBay) be suppressed on retrial. Instead, the court reversed Guidry's conviction on alternative grounds, thus declining to articulate any particularity requirements. It is only a matter of time until the question hits the court's dockets again.

Other jurisdictions have adopted minimization procedures that the court should consider and adopt.

The court need not wait for an appeal to set such requirements. Prophylactic action via a change in court rules, *see* Nev. Const. Art. 6 § 4; NRS 2.120, seems preferrable, allowing time and opportunity to review actions taken by other jurisdictions and weigh the benefits and burden of each. *See* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 Emory L.J. 49, 82 (2018) (discussing and weighing the benefits of minimization procedures taken by various courts). In its answering brief in *Guidry*, the state suggested that it was impossible for it to provide any greater specificity as to the electronic data it sought to search and seize. No. 80156 Respondent's Answering Brief at 80. But other jurisdictions have successfully set judicial guidelines on electronic searches that minimize the state's intrusion on privacy rights.

Some jurisdictions have implemented protocol for cell phone searches, requiring the state to detail, ex ante, the steps it will take to search the electronic device. Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585, 591 (2016) (collecting cases); *see In re Search of premises known as Three Cellphones & One Micro-SD Card*, No. L4-MJ-8013-DJW, 2014 WL 3845157, at *2 (D. Kan. Aug. 4, 2014). The court could similarly require that the state describe what process it will implement to "separate[e] seizable data (as defined by the warrant) from all other data. … [I]f [for example] the government is allowed to seize information pertaining to ten names, the search protocol should be designed to discover data pertaining to those names only, not to others, and

CONTINUED ON PAGE 25

CONTINUED FROM PAGE 23

Preventing Overcollection of Electronic Information

not those pertaining to other illegality." *CDT*, 621 F.3d 1162, 1179 (Kozinsky, J. concurring).

The court might follow other jurisdictions that require the state to specify where on a digital device it intends to look for evidence. *See* Gershowitz, *supra* at 91 (collecting examples). If, for example, the crime charged is vehicular homicide, and based on the driver texting while driving, the state should limit its request to search to the driver's text application, and only for activity occurring at the relevant time.

In the event the state is truly unable to provide any of the additional details noted above, the court could instruct "magistrate judges [to] insist that the government forswear reliance on the plain view doctrine." *CDT*, 621 F.3d at 1178. With such a protection in place, at least some of the sting of an otherwise overbroad search and seizure is neutralized. And, as a backstop, the court might also consider a rule requiring the state to "destroy or, if the recipient may lawfully possess it, return non-responsive data" within a certain period. *Id.* at 1180. This requirement would ensure that citizens' digital lives are not permanently upended following a search warrant.

In sum, the court should clearly delineate the specificity required for a valid warrant for an electronic search, examining and adopting minimization techniques used by other courts. To best protect the rights of Nevada's citizens—whether individual and corporate—the court would be justified in (and seemingly better-served by) addressing the issue head-on, via court rule.

LAUREN WIGGINTON is an appellate and litigation attorney at Lewis Roca Rothgerber Christie LLP. Before joining Lewis Roca, she served as a judicial clerk on the Nevada Supreme Court, litigation attorney at a national law firm, and staff attorney with the Nevada Supreme Court. Wigginton earned her B.A. and J.D. at University of California, Davis.

ENDNOTE:

1. The article uses the phrase "electronic searches" to describe searches of electronic storage mediums, including computer hard-drives, cellphones, and third-party servers.