



CIRCUIT COURT OF THE STATE OF OREGON
FOURTH JUDICIAL DISTRICT
MULTNOMAH COUNTY COURTHOUSE
1021 SW FOURTH AVENUE
PORTLAND, OR 97204-1123

BRONSON D. JAMES
JUDGE

PHONE (503) 988-5544
Bronson.D.James@oid.state.or.us

GUIDELINES FOR APPLYING FOR A DATA WARRANT

This document is meant as a guide to affiants applying to Judge James for a warrant for data. As each warrant is judged on its own unique circumstances, this document will not apply in every case, but is offered as a general guideline for the typical data warrant. This document is not a litmus test, nor a checklist. Not every point in the guidelines may be practicable in every warrant affidavit.

Overview

Because of the nature and extent of personal data contained on phones and other portable electronics, the privacy interest is the equivalent of (and arguably greater than) a residence. *Riley v. California*, ___ US ___, 134 S Ct 2473, 2484, 189 L Ed 2d 430 (2014).

Warrant affidavits, and the issuing warrant, must describe, with particularity the data to be seized, and searched. ORS 133.535 lists permissible objects of a search or seizure as “(1) Evidence of or information concerning the commission of a criminal offense . . . (3) Property that has been used, or is possessed for the purpose of being used, to commit or conceal the commission of an offense.”

ORS 133.545 sets out issuance requirements, including the requirement that the affidavit offered in support of the warrant application state with particularity those facts thought to establish probable cause to search: “(4) The application shall consist of a proposed warrant in conformance with 133.565, and shall be supported by one or more affidavits

particularly setting forth the facts and circumstances tending to show that the objects of the search are in the places, or in the possession of the individuals, to be searched. . . .”

Similarly, ORS 133.565 sets out the required contents of a warrant, including the need for particularity in the description of the objects of the search and the things to be seized as follows: “(1) A search warrant shall be dated and shall be addressed to and authorize its execution by an officer authorized by law to execute search warrants. (2) The warrant shall state, or describe with particularity . . . (c) the things constituting the object of the search and authorized to be seized . . .”

The statutory requirement for particularity reflects the requirements under both Article I, section 9 of the Oregon Constitution and the Fourth Amendment to the United States Constitution. *State v. Farrar*, 309 Or 132, 786 P2d 161 (1990) and *State v. Hodges*, 43 Or App. 547, 603 P2d 1205 (1979); see also *Lo-Ji Sales, Inc. v. New York*, 442 US 319, 325, 99 S Ct 2319, 60 L Ed 2d 920 (1979) (finding the Fourth Amendment was designed to protect us from the 18th century general warrant or writ of assistance, among other things).

To be sufficient, an affidavit in support of a warrant must permit a conclusion by a neutral and detached magistrate that the items specified in the warrant will probably be found in a specified place to be searched. ORS 133.555(2). The standard is one of probability, which requires more than a mere possibility, *State v. Carter/Grant*, 316 Or 6, 13, 848 P2d 599 (1993).

An officer's training and experience are to be accorded some weight, but there must be other facts establishing the required nexus. *State v. Beagles*, 143 Or App 129, 136, 923 P2d 1244 (1996).

While an officer's "expertise" may contribute to a probable cause showing by providing "a criminal law nexus" to facts that "could be [otherwise] understood to be innocent," to demonstrate probable cause, the affidavit must first provide "separately verified facts" linking the offense under investigation to the thing to be searched. *State v. Goodman*, 328 Or 318,327, 975 P2d 458 (1999).

For example, if an officer avers that his training and experience have taught him that “paperfolds of a particular shape are often used for drugs,”

and the officer also testifies that “the defendant possessed a paperfold of that particular shape,” the training and experience create “a basis to believe that the defendant's paperfold contained drugs.” *State v. Miglavs*, 186 Or App 420, 432, 63 P3d 1202 (2003), *aff'd*, 337 Or 1, 90 P3d 607 (2004) (citing *State v. Herbert*, 302 Or 237, 242, 729 P2d 547 (1986)).

As the Oregon Court of Appeals has summarized, “the training and experience information (paperfolds contain drugs) supplies the major premise on which the conclusion (defendant possessed drugs) depends, and that major premise must be followed by a minor premise (defendant possessed a paperfold) that is supported by objective facts derived from other sources.” *State v. Daniels*, 234 Or App 533, 540–41, 228 P3d 695, 699–700 (2010).

In the context of data searches, “training and experience” that computers and cellphones contain significant information about communications, location, potential pictures of criminal activity, etc., is the major premise. But the affidavit still requires the minor premise, namely some specific and articulable objective fact related to the case at hand that ties the computer or phone to the criminal investigation.

First Guideline – Specify the Type of Data to be Searched

Requests to “search the cell phone” are not sufficiently particular. Affiants should state the type of data for which probable cause exists. For example:

- | | |
|--|---|
| <input type="checkbox"/> Image Files | <input type="checkbox"/> Document files |
| <input type="checkbox"/> Video Files | <input type="checkbox"/> Image Files |
| <input type="checkbox"/> Email | <input type="checkbox"/> Text communication |
| <input type="checkbox"/> Call records | <input type="checkbox"/> Voicemail |
| <input type="checkbox"/> Browser history | <input type="checkbox"/> Contacts |
| <input type="checkbox"/> Other _____ | <input type="checkbox"/> Other _____ |

Each type of data should be separately called out, such that the affidavit and subsequent warrant clearly set forth what type of data is, and is not, subject to search.

Second Guideline – Limit the Timeframe

Because of the vast storage capacity of digital media, a cellphone can hold years worth of data. Because there is rarely probable cause for years worth of data, affiants are encouraged to limit the data search to a reasonable time frame, typically not in excess of thirty days surrounding the date of alleged the criminal activity. Thirty days is not a *per se* legitimate timeframe; a more targeted period may be appropriate. Note that the reasonable timeframe may not be the same for each type of data sought.

Limiting the timeframe will often result in a series of supplemental warrants being sought. For example, the initial warrant may authorize a search for thirty days of data, which generates new specific and articulable facts supporting probable cause for a new date range, and generates a supplemental warrant affidavit.

Third Guideline – State How the Search Will Be Conducted

Searches of data, such as cellphones, typically occur in one of two ways, either direct search of a device, or through imaging the drive then searching the image. Affiants need to specify how the search will be conducted, as this affects what the warrant needs to contain.

It is helpful for the affidavit to state where the data search will be conducted, by whom, and the names and general descriptions of devices and/or algorithms used for imaging and searching.

Fourth Guideline – Remote Data

Some data is not stored on the phone locally, but the phone is a conduit to remotely stored information. Social media applications for example often store the data remotely, and the phone is just a gateway to that data. The affiant should specify if they want to use the device to access remote data, for example, opening the Facebook app on a seized cellphone.

Because remote data can be obtained via a warrant to the remote data host, the affiant should explain why a warrant to Facebook for example is not possible or practicable in this case.

Fifth Guideline – Timeframe for Search

A warrant for a data search issued by the court will typically require that the search be conducted within thirty days of the seizure of the device. The affiant is advised to justify a later timeframe if one is sought.

Sixth Guideline – Non Responsive Data

Given the capacity of digital storage devices, when a device is imaged only a small fraction of the data copied will bear a connection to the crime of investigation. The vast bulk of copied data is non-responsive, and there is no probable cause for a continued seizure of that data. Affiants must therefore be prepared to describe how that non-responsive data will be purged from governmental control, and in what timeframe.

In addition, the affiant should explain how the search will be conducted so as to comply with ORS 133.539, 163.633, 163.643, and 163.653, which provide that forensically imaged raw data must be able to be returned pursuant to an order for return of seized property. ORS 163.653 (3)(a), “An order granting a motion for return of raw data obtained from the forensic imaging of a portable electronic device or of a computer shall include a provision that a law enforcement agency may not retain a copy of the raw data to be returned.” In particular, the affiant should affirm that forensic images will not be shared with any law enforcement agencies that would be beyond the reach of an order for return of data from this court.

///

Conclusion

These guidelines are developed through a review of caselaw and scholarly work nationwide, and are intended to help affiants and the court in constructing warrants that enable law enforcement investigation while protecting the constitutional privacy rights in digital data. These guidelines are not controlling, and affidavits and warrants that fail to comply with these guidelines are not presumptively invalid.



Hon. Bronson D. James
Circuit Court Judge
Multnomah County Courthouse
1021 SW Fourth Avenue
Portland, OR 97204
503.988.5544

First Draft: July 1, 2016

Edited: August 8, 2016