Golden Gate University Law Review

Volume 40
Issue 3 *Ninth Circuit Survey*

Article 3

January 2010

United States v. Payton: Redefining the Reasonableness Standard For Computer Searches and Seizures

Susan A. Rados

NOTE

UNITED STATES V. PAYTON: REDEFINING THE REASONABLENESS STANDARD FOR COMPUTER SEARCHES AND SEIZURES

INTRODUCTION

Imagine a scenario where officers arrive at a residence to execute a search warrant in which evidence of drug use and documents indicating drug trafficking are sought. The officers search the home and find evidence of drug use but no documents related to drug sales. They enter the bedroom and find both a file cabinet and a computer. Based upon the officers' experience and training, they know that both the file cabinet and the computer could contain items enumerated on the warrant – one in paper form and the other in digital form. Neither the file cabinet nor the computer is listed on the warrant, nor, the officers believe, is such a listing required for them to search either one. Under traditional Fourth Amendment jurisprudence, the officers can look in any container where the items they seek could reasonably be expected to be found. The Fourth Amendment makes no distinction between a computer and a file cabinet, but the United States Court of Appeals for the Ninth Circuit now does.

United States v. Payton[1] held that officers may not seize or search a computer unless there are "circumstances indicating a likelihood" that the officers will find the evidence they seek on that

[1] United States v. Payton, 573 F.3d 859 (9th Cir. 2009).

particular computer.[2] In its holding, the court distinguished traditional containers, such as file cabinets, from computers, holding that, in contrast to the rule applicable to a traditional container, it is not enough that the computer "could" contain the evidence; rather, there must be some showing that the computer "would" contain the evidence.[3] This creates an impractical constraint upon searches and seizures of computers and is contrary to U.S. Supreme Court precedent and the Fourth Amendment.[4] *Payton* further marks a change in direction from previous Ninth Circuit decisions by approaching what appears to be a bright-line rule, namely that officers may not search a computer without a warrant.[5] If a computer search is not authorized on the original warrant, officers must demonstrate "circumstances indicating a likelihood" that what they are looking for would be found in a particular computer.[6] In turn, this would allow the officers to secure the computer while applying for a subsequent warrant to search the computer.[7] Even as the Ninth Circuit presumably intended to protect constitutional privacy interests by changing the reasonableness standard in computer searches from "could" to "would," the unintended results will likely have the opposite effect. The most likely result is this: So long as the evidence they are seeking could be found in digital form, the officers will simply request authorization, in the initial warrant, to search any computer they might find. By doing so, they will – in the event they find a computer in their initial search – avoid having to seek a subsequent warrant by demonstrating circumstances that implicate that particular computer. This unintended consequence will weaken the Ninth Circuit's effort to protect individual constitutional privacy in the context of computer searches and seizures.

This Note examines *United States v. Payton* and the issue of when it is reasonable to search a computer if it is not expressly authorized on the search warrant. Part I discusses the background facts of *Payton* and the Fourth Amendment. Part II analyzes why the Ninth Circuit ultimately decided *Payton* correctly but focused on the wrong underlying reason in its holding. The

---

[2] *Id*. at 863.

[3] *Id.* at 863.

[4] *See* United States v. Ross, 456 U.S. 798, 823 (1982).

[5] *Payton*, 573 F.3d at 863-64.

[6] *Id.* at 863.

[7] *Id*.

reasonableness standard for computer searches should be whether the computer "could" contain the evidence, rather than the stricter standard of "would" contain the evidence announced in *Payton*. However, because computers are different from traditional containers, they should be subject to judicial supervision and a defined search protocol as expressed through a warrant. Part III explains how the Ninth Circuit in *Payton* ultimately did what it had said it would not do in *United States v. Giberson*: create a distinctive category for computers separate from traditional containers and imply a bright-line rule mandating that a computer may not be searched without a warrant.[8] Part IV proposes a practical reasonableness standard that balances the special needs of a computer search with the flexibility found under traditional container theories of searches and seizures. This Note proposes a specific set of guidelines to establish a protocol for properly seizing a computer that will effectively balance the government's interest in searching and seizing a computer with the computer owner's privacy interests.

I. BACKGROUND

This Part starts by looking at the facts of *United States v. Payton* and the two issues the Ninth Circuit addressed: the validity of the search warrant and its scope.[9] The second section of this Part provides a general background of Fourth Amendment law and a discussion of probable cause and the scope of a warrant.[10]

A. FACTS AND HISTORY OF *UNITED STATES V. PAYTON*

On July 30, 2004, Officer Jeffrey R. Horn requested a search warrant for a residence in Merced, California, based on suspicion of drug trafficking and drug use.[11] The warrant contained "Attachment A," which listed all drug-related items to be seized, including "[s]ales ledgers showing narcotics transactions such as pay/owe sheets"[12] and "[f]inancial records of the person(s) in control of the residence or premises, bank accounts, loan

[8] United States v. Giberson, 527 F.3d 882 (9th Cir. 2008).

[9] *Payton*, 573 F.3d at 861.

[10] *Id.*

[11] Opening Brief of Appellant at 5, United States v. Payton, 573 F.3d 859 (9th Cir. 2009) (No. 07-10567), 2007 WL 5108020.

[12] *Payton*, 573 F.3d at 860.

applications, [and] income and expense records."[13]

In the affidavit asserting probable cause, Officer Horn requested permission to search any computers in the residence,[14] even though he had no specific basis on which to believe that a computer would be found in the house.[15] He stated, based on his experience and training, that drug dealers "maintain evidence of sales of narcotics on their computers."[16] He further requested that the warrant "allow [him] to look at computer files, and seize the computer if it shows evidence of criminal behavior."[17] The request to search any computers in the residence was inadvertently left off of "Attachment A,"[18] and the magistrate authorized the police to search only those items listed.[19]

During the execution of the warrant, officers seized a small quantity of methamphetamine as well as several pipes that appeared to be the type used to smoke controlled substances.[20] The officers also found evidence of marijuana leaves and seeds on the floor of the master bedroom, which the officers determined to be that of Michael Payton.[21] While searching the master bedroom, Officer Horn found a computer that he noted to be in screen-saver mode.[22] Officer Horn moved the mouse to deactivate the screen saver; thereafter, the screen showed a list of computer files and he clicked on the first one.[23] The file opened to reveal what appeared to be a naked 10-year-old girl lying on a bed with her legs spread apart.[24] Officer Horn believed the image to be child pornography, closed the file, and seized the computer.[25] The officers found no evidence of drug sales in the residence.[26]

Michael Payton was charged with possession of child pornography[27] and moved to suppress the evidence on two

---

[13] *Id.*

[14] Opening Brief of Appellant, *supra* note 11, at 5.

[15] *Id.* at 8.

[16] Brief for Appellee at 7, *Payton*, 573 F.3d 859 (No. 07-10567), 2008 WL 2623359.

[17] Opening Brief of Appellant, *supra* note 11, at 8.

[18] Brief for Appellee, *supra* note 16, at 7.

[19] Opening Brief of Appellant, *supra* note 11, at 6.

[20] Brief for Appellee, *supra* note 16, at 7.

[21] *Id.*

[22] *Id.*; United States v. Payton, 573 F.3d 859, 860 (9th Cir. 2009).

[23] Brief for Appellee, *supra* note 16, at 8.

[24] *Id.*

[25] *Id.*; *Payton*, 573 F.3d at 860.

[26] *Payton*, 573 F.3d at 860.

[27] Michael Payton was charged with a violation of 18 U.S.C. § 2252(a)(4)(B), which

grounds.[28] He argued that the warrant lacked probable cause and that the search of the computer exceeded the scope of the warrant.[29] The district court denied the motion to suppress the evidence, finding that the warrant was based upon sufficient probable cause, and ruled that the defect of failing to list the computer listed on "Attachment A" was cured by the magistrate's subsequent testimony that he had intended to authorize a search of computers.[30]

1. Probable Cause for the Search Warrant

The Ninth Circuit agreed with the district court's ruling that the warrant was based upon sufficient probable cause.[31] Officer Horn stated in his affidavit for probable cause that neighbors had complained of drug sales.[32] However, during a *Franks*[33] hearing, Officer Horn testified that he knew of no neighbors complaining of drug sales, only of one neighbor complaining of drug use.[34] Officer Horn had inferred from the complaint of drug use that probable drug sales were going on.[35] Further, Officer Horn testified that he relied on the fact that during the previous arrest of

---

states that any person who

> knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if--
> (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
> (ii) such visual depiction is of such conduct;
> shall be punished as provided in subsection (b) of this section.

18 U.S.C.A. § 2252(a)(4)(B) (Westlaw 2010).

[28] *Payton*, 573 F.3d at 860.

[29] *Id.*

[30] *Id.* at 861.

[31] *Id.* The district court found that "'even if [it] excised and consider[ed] the entire warrant without a complaint of neighbors of drug sales,' the warrant was still sufficient in light of the other evidence presented." *Id.*

[32] *Id.* at 860.

[33] Franks v. Delaware, 438 U.S. 154, 171-72 (1978). In a *Franks* hearing, a defendant can challenge the validity of a facially valid warrant by contesting assertions made in the affidavit upon which the warrant was issued. The warrant will be considered invalid if the defendant can substantially show: 1) a false statement was included in the affidavit, 2) the false statement was necessary to find probable cause, and 3) the affiant knowingly or recklessly included the false statement.

[34] Opening Brief of Appellant, *supra* note 11, at 8.

[35] *Id.*

another resident of the home, he and his fellow officers had found 2.7 grams of methamphetamine pinned to the inside of her bra.[36] The fact that the drugs were divided into two separate bags, as well as the quantity involved, led Officer Horn to believe the resident possessed the drugs for sale.[37] This Case Note will not address the issue of probable cause for the warrant and the reasoning behind the court's finding at the *Franks* hearing but will instead focus on the scope of the warrant.

2. Scope of Warrant

In addition to challenging the probable cause supporting the warrant, Michael Payton argued that the search of the computer exceeded the scope of the warrant because the warrant did not authorize the search and seizure of *any* computers.[38] However, the district court held that the search of the computer was valid "because the failure to include the word 'computers' in Attachment A was an oversight cured by the issuing judge's testimony of his intent."[39]

The Ninth Circuit disagreed with the district court. The Ninth Circuit concluded that after-the-fact testimony could not cure the search warrant's lack of the word "computers."[40] Merced County Superior Court Judge John Kirihara testified at the federal evidentiary hearing regarding the issuance of the warrant, stating that he often asks officers to add items to the Attachment that they may have missed.[41] He did not do so in this case and only authorized those items listed.[42] Judge Kirihara noted, however, that he was aware Officer Horn had requested permission to search computers and that he had intended to authorize that search.[43] Neither Officer Horn nor Judge Kirihara noticed that the word "computers" was missing from Attachment A.[44]

The Ninth Circuit held that this after-the-fact testimony did not provide the authorization necessary to search computers, since "one purpose of a warrant is to inform the person subject to the

[36] *Id.* at 7.
[37] Brief for Appellee, *supra* note 16, at 5.
[38] Opening Brief of Appellant, *supra* note 11, at 11.
[39] United States v. Payton, 573 F.3d 859, 861 (9th Cir. 2009).
[40] *Id.* at 862.
[41] Opening Brief of Appellant, *supra* note 11, at 6.
[42] *Id.*
[43] *Id.* at 6-7.
[44] *Id.* at 7.

search just what may be searched."[45] Upon this holding, the Ninth Circuit's analysis turned to Fourth Amendment jurisprudence concerning the circumstances in which a computer may be seized and searched absent express authorization in a search warrant.

B. RELEVANT FOURTH AMENDMENT LAW

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[46]

The Fourth Amendment was adopted in 1791 in response to the English practice of issuing general warrants against political suspects, and the colonial practice of issuing writs of assistance against those suspected of smuggling goods.[47] The general warrant and the writ of assistance gave executing officers authority to search without limitation[48] and allowed "a general, exploratory rummaging in a person's belongings."[49] To curtail these general warrants and writs of assistance, the Fourth Amendment prohibited unreasonable searches and seizures. [50]

The Fourth Amendment applies to searches or seizures under two conditions. First, the government must be performing the search or seizure.[51] The Fourth Amendment does not protect a search or seizure performed by a private actor.[52] Second, a person must have a justifiable expectation of privacy in the intruded-upon area.[53] This requires the person whose property is searched or seized to have both a subjective expectation of privacy as well as an objective one "that society is prepared to

---

[45] *Payton*, 573 F.3d at 862 (citing United States v. Hayes, 794 F.2d 1348, 1355 (9th Cir. 1986)).

[46] U.S. CONST. amend. IV.

[47] Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 HARV. L. REV. 361, 361-64 (1921).

[48] *Id.* at 361.

[49] Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

[50] Fraenkel, *supra* note 47, at 366.

[51] Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

[52] *Id.*

[53] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

recognize as reasonable."[54]

In *Katz v. United States*, the FBI attached an electronic listening device to the outside of a public telephone booth and recorded a conversation.[55] The United States Supreme Court determined that Katz had a subjective expectation of privacy when he entered the telephone booth and placed his phone call, based on the rationale that he had no reason to believe his conversation would be overheard.[56] In addition, the Supreme Court determined that Katz had an objective expectation of privacy,[57] holding that while a public telephone booth provides no expectation of privacy in what can be seen, there is an expectation of privacy in what can be heard.[58]

A governmental search or seizure of property in which a person has a subjective and objective expectation of privacy violates the Fourth Amendment if it is "unreasonable."[59] The Supreme Court has explained that reasonableness is determined by "balancing [the] intrusion on the individual's Fourth Amendment interests against [the] promotion of legitimate governmental interests."[60] The search or seizure is reasonable if it is authorized by a valid warrant or if it fits in one of the warrant exceptions.[61]

In a warrant situation as in *Payton*, a neutral magistrate judge conducts the balancing test and determines whether a search warrant will be issued.[62] The search warrant must (1) be based

---

[54] *Id.* at 361.

[55] *Id.* at 348 (majority opinion).

[56] *Id.* at 352.

[57] *Id.*

[58] *Id.*

[59] U.S. CONST. amend. IV.

[60] Delaware v. Prouse, 440 U.S. 648, 654 (1979).

[61] There are limited circumstances in which officers may conduct a search or seizure without a warrant. These include the following: searches that are incident to a lawful arrest, United States v. Robinson, 414 U.S. 218, 224 (1973); searches of automobiles when officers have probable cause to believe instrumentalities of crime, evidence, or contraband are within the automobile, Carroll v. United States, 267 U.S. 132, 149 (1925); seizures of contraband when it is in plain view of an officer, Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971); searches of people whom the police have an articulable suspicion to believe are involved in criminal activity, Terry v. Ohio, 392 U.S. 1, 21 (1968); searches of places and things when the officers are given consent by a person with authority to consent, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973); and searches and seizures due to exigent circumstances. Exigent circumstances include hot pursuit of a fleeing felon, Warden v. Hayden, 387 U.S. 294, 310 (1967), reason to believe that evidence will be destroyed before a warrant can be obtained, Schmerber v. California, 384 U.S. 757, 770 (1966), and reason to believe someone may be in imminent danger, Brigham City v. Stewart, 547 U.S. 398, 406 (2006).

[62] Coolidge v. New Hampshire, 403 U.S. 443, 449 (1971).

upon probable cause and supported by oath or affirmation, and (2) particularly describe the places to be searched and the items to be seized.[63] The language of the warrant determines the scope of the search, which in turn is based on an objective standard of reasonableness.[64]

1. Search Warrant's Probable-Cause Determination

Probable cause is a fluid concept that does not deal with hard certainties.[65] It exists when facts and circumstances would lead a reasonable person to conclude that seizable evidence would be found on the premises or person to be searched.[66] Whether there is sufficient information to give rise to probable cause is based on the totality of the circumstances.[67] Under this approach, the relative weights of all indicia of reliability can be assessed and balanced.[68] Under this standard, no single piece of evidence need be conclusive. Rather, everything is examined in light of the other facts. Accordingly, an officer wishing to apply for a search warrant must prepare an affidavit outlining the facts[69] that cause the officer to believe the evidence sought would be at the time and place that the search is to be conducted.[70]

An officer may prepare an affidavit based entirely on hearsay,[71] such as testimony by a victim of crime, witnesses, or police informants. In using hearsay information, the affidavit must show that the informant is reliable and has a basis of knowledge for the information.[72] The affidavit is then presented to a neutral magistrate, who makes an independent evaluation as to whether there is sufficient probable cause.[73]

2. Particularity Requirement

"The Fourth Amendment's specificity requirement prevents

---

[63] U.S. CONST. amend. IV.

[64] United States v. Leon, 468 U.S. 897, 920-21 (1984).

[65] Carroll v. United States, 267 U.S. 132, 161 (1925).

[66] *Id.*

[67] Illinois v. Gates, 462 U.S. 213, 252 (1983) (White, J., concurring in judgment).

[68] *Id.* at 234 (majority opinion).

[69] Affidavits must consist of facts and not conclusions. *See* Aguilar v. Texas, 378 U.S. 108, 114 (1964).

[70] *Gates*, 462 U.S. at 238.

[71] *Id.* at 242.

[72] *Id.* at 227.

[73] United States v. Ventresca, 380 U.S. 102, 109 (1965).

officers from engaging in general, exploratory searches by limiting their discretion and providing specific guidance as to what can and cannot be searched and seized."[74] This requirement prevents what may amount to a fishing expedition. As the Supreme Court explained:

> By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the 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.[75]

Therefore, the more detailed and specific the descriptions of the items to be seized on the warrant are, the more limited the search will be, and the more likely the warrant will be upheld as constitutional.

A warrant is deemed unconstitutional if it does not describe with sufficient particularity the place to be searched and the items to be seized, even if the affidavit itself is sufficiently particularized.[76] However, the warrant need only be "reasonably specific, rather than elaborately detailed,"[77] "and the specificity required 'varies depending on the circumstances of the case and the type of items involved.'"[78] For example, a warrant authorizing the seizure of accounting-related documents like ledgers, bank records, and spreadsheets would likely satisfy the particularity requirement. However, the description of accounting-related documents does not have to be exact.[79]

---

[74] United States v. Adjani, 452 F.3d 1140, 1147 (9th Cir. 2006).

[75] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[76] Groh v. Ramirez, 540 U.S. 551, 557 (2004).

[77] United States v. Rude, 88 F.3d 1538, 1551 (9th Cir. 1996) (quoting United States v. Brock, 667 F.2d 1311, 1322 (9th Cir. 1982)).

[78] *Rude*, 88 F.3d at 1551 (quoting United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)).

[79] The Ninth Circuit considers three factors in determining whether a warrant meets the particularity requirement:

> (1) [W]hether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.

United States v. Lacy, 119 F.3d 742, 746 n.7 (9th Cir. 1997) (quoting United States v. Noushfar, 78 F.3d 1442, 1447 (9th Cir. 1996)).

3. The Scope of a Search Is Based on an Objective Standard of Reasonableness

The scope of a search warrant is based on an objective standard determined by the language of the warrant, without regard to the subjective intent of the executing officers or the issuing magistrate judge.[80] Thus, "[a] policeman's pure heart does not entitle him to exceed the scope of a search warrant, nor does his ulterior motive bar a search within the scope of the warrant, where the warrant was properly issued."[81] The objective standard of reasonableness must guide the officer in his or her search.[82]

In using an objective reasonableness standard, the officer cannot look for an object in places smaller than the object authorized by the warrant.[83] However, once an officer finds a container that may conceal the object authorized by the warrant, the container may be opened immediately.[84] The Supreme Court justified this by stating that "the individual's interest in privacy must give way to the magistrate's official determination of probable cause."[85]

Moreover, there is no Fourth Amendment distinction between traditional containers that are readily accessible and those that are locked.[86] Once again, the courts have held that the driving factor is one of "reasonableness."[87] If it is reasonable to believe a container may have evidence within it, the officer may take measures to open it.[88] An officer does not need to seek a separate warrant to search a locked container if he or she is working within the scope of the original warrant.[89] As the Fifth Circuit has explained, to hold otherwise would

> require either that "an additional search warrant (be obtained) for each container within a larger container," or that the agent seeking the warrant possess extrasensory perception so that he

---

[80] Whren v. United States, 517 U.S. 806, 813 (1996).

[81] United States v. Ewain, 88 F.3d 689, 694 (9th Cir. 1996).

[82] Scott v. United States, 436 U.S. 128, 137 (1978).

[83] United States v. Ross, 456 U.S. 798, 824 (1982).

[84] *Id.* at 823.

[85] *Ross*, 456 U.S. at 823.

[86] United States v. Gomez-Soto, 723 F.2d 649, 654-55 (9th Cir. 1984) (citing United States v. Morris, 647 F.2d 568, 573) (5th Cir. 1981)).

[87] *See, e.g.*, United States. V. Gomez-Soto, 723 F.2d 649 (9th Cir. 1984); United States v. Morris, 647 F.2d 568 (5th Cir. 1981).

[88] *Id.*

[89] *Id.*

> could describe, prior to entering the house, the specific boxes, suitcases, sofas, closets, etc. that he anticipated searching. Obviously, neither alternative is either reasonable or required.[90]

This holds true even if the container cannot be opened on the premises and must be removed to be opened.[91]

II. *PAYTON* REACHED THE RIGHT RESULT BUT FOCUSED ON THE WRONG REASON

In *Payton*, the Ninth Circuit suppressed the evidence obtained from the computer for two reasons. First, the search of the computer was unreasonable.[92] Second, the search was not authorized by a warrant.[93] However, in reaching its conclusion, the court followed *Giberson* and changed the standard of reasonableness from one requiring only that the evidence *could* be found in the computer to one requiring circumstances that indicate the evidence *would* be found in the computer.[94]

In doing so, the Ninth Circuit departed from Supreme Court precedent[95] in container searches and applied an impractical reasonableness standard. In its holding, the court states that absent evidence implicating the computer, a computer cannot be seized (and by implication, a subsequent warrant will not issue).[96] Since in *Payton* there were no circumstances indicating a likelihood that the evidence would be found in the computer, the court held that the search of the computer was unreasonable.[97]

The Ninth Circuit should only have considered whether the items *could* have been found on the computer and the fact that a

---

[90] United States v. Morris, 647 F.2d 568, 573 (5th Cir. 1981) (citation omitted) (quoting United States v. Kralik, 611 F.2d 343, 345 (10th Cir. 1979)).

[91] United States v. Johnson, 709 F.2d 515, 516 (8th Cir. 1983) (locked safe reasonably believed to contain items enumerated in warrant was permissibly moved to police station where it could be opened).

[92] United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).

[93] *Id.*

[94] *Id*. at 862-63 (quoting United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008)).

[95] United States v. Ross, 456 U.S. 798, 823 (1982).

[96] In *United States v. Giberson*, the court held that, absent "evidence" implicating the computer, a seizure of Giberson's computer would not have been reasonable. *Giberson*, 527 F.3d at 887. In *United States v. Payton*, the court applied the same standard to the search of a computer and reasoned that "the special considerations of reasonableness involved in the search of computers are reflected in the practice . . . of searching officers to *stop and seek an explicit warrant* when they encounter a computer that they have reason to believe should be searched." *Payton*, 573 F.3d at 864 (emphasis added).

[97] *Payton*, 573 F.3d at 863.

subsequent warrant for the computer was not obtained. Even though it was reasonable for the officer to suspect that the computer contained the items he sought, by not obtaining a warrant for its search, he acted in the absence of judicial supervision and without an approved search protocol. This reasoning would still have allowed the court to suppress the evidence while retaining a reasonableness standard consistent with Supreme Court precedent.

This Part begins by explaining the Ninth Circuit's basis for suppressing the evidence. Next, this Part analyzes the reasonableness standard set forth in *Payton* and discusses why this rule is impractical and will likely have unintended consequences. This requires a journey back to *United States v. Giberson*, the prior precedent-setting case on search warrants and computers. This also requires a brief survey and comparison of other jurisdictions' standards on this issue. This Part concludes with an analysis of the differences between a computer and a traditional container and why there should be different search protocols for each of them.

A. NINTH CIRCUIT'S BASIS FOR SUPPRESSING THE EVIDENCE

The Ninth Circuit found the actions of the officers in *Payton* unreasonable for two reasons. First, in the course of Officer Horn's search, he did not find evidence to support his conclusion that the computer he found contained items enumerated in the warrant.[98] Instead, Officer Horn relied on the fact that the evidence he sought *could* be found on a computer.[99] In its analysis, the court applied the stricter "would" standard it first enunciated in *Giberson*[100] and found that the facts of *Payton* did not meet that standard.[101]

In *Giberson*, agents had a search warrant to look for, among other things, evidence pertaining to identity theft.[102] Upon executing the warrant, the officers discovered a personal computer on a desk in one of the bedrooms.[103] The computer was

---

[98] *Payton*, 573 F.3d at 864.

[99] *Id.* at 863 (recognizing that pay/owe sheets are physically capable of being kept on a computer).

[100] *Giberson*, 527 F.3d at 887.

[101] *Payton*, 573 F.3d at 684.

[102] *Giberson*, 527 F.3d at 884.

[103] *Id.*

connected to a printer located on an adjacent dresser.[104] On the dresser were "what appeared to be fake Nevada I.D. cards" that seemed to have been printed from the printer.[105] Upon searching the desk and surrounding area, the agents found documents "evidencing the production of false I.D.s, including fake Social Security cards and State of New York birth certificates . . . ."[106] The officers then seized the computer and secured a second search warrant to search the computer itself.[107]

The *Payton* court approved of the officers' actions in *Giberson* and applied the same analysis to *Payton*.[108] In *Payton*, the court reiterated *Giberson*'s rule of reasonableness: "If it is reasonable to believe that a computer contains items enumerated in the warrant, officers may search it."[109] While this appears fairly broad in scope, the court went on to narrow its position and reiterated the new reasonableness standard it created in *Giberson*, stating that "*where there was ample evidence that the documents in the warrant could be found on Giberson's computer*, the officers did not exceed the scope of the warrant when they seized the computer."[110] The *Payton* court applied the same reasonableness standard it used to approve the seizure of Giberson's computer to the search of Payton's computer.[111] The court concluded there was an absence of "legitimating facts" in *Payton*.[112]

Second, the court expressed disapproval of the fact that Officer Horn chose to search the computer first, before seeking a second warrant authorizing the search.[113] This was in contrast to the actions of the agent in *Giberson*, who seized the computer first, and then sought a warrant before the search.[114]

---

[104] *Id.*
[105] *Id.*
[106] *Giberson*, 527 F.3d at 884-85.
[107] *Id.* at 885.
[108] United States v. Payton, 573 F.3d 859, 863 (9th Cir. 2009).
[109] *Payton*, 573 F.3d at 864 (quoting *Giberson*, 527 F.3d at 888).
[110] *Id.* at 863 (emphasis in original).
[111] *Id.* at 862-63.
[112] *Id.* at 864.
[113] *Id.* at 863.
[114] *Id.*

B. THE STANDARD FOR REASONABLENESS IN SEARCHING COMPUTERS SHOULD BE THE SAME STANDARD AS FOR OTHER TRADITIONAL CONTAINERS

The reasonableness standard set forth by the Ninth Circuit in *Payton* is impractical. The officers in *Payton* were looking for documents that could reasonably be found in a computer. In today's society, most people create spreadsheets on their computers and download bank records directly to their computers. As a result, a computer would be a reasonable place to search for items such as pay/owe sheets and other financial documents. Therefore, it was reasonable for the officer in *Payton* to believe the computer was a place where the items in the warrant could be found.

The Ninth Circuit distinguished *Payton* from *Giberson*, noting that, unlike the agents in *Giberson*, the officers in *Payton* found nothing to indicate a likelihood that the computer contained the evidence for which they were looking.[115] The court again reiterated its position on reasonableness, stating that it is not enough that the evidence is *capable* of being contained in a computer.[116] In order for a search to be reasonable, there must be "circumstances indicating a likelihood" that the items to be seized are contained in the computer.[117]

Apart from the specific facts provided in *Giberson*, the Ninth Circuit has offered very little guidance as to how "circumstances indicating a likelihood" should be interpreted. There is no indication of how strong a likelihood is needed, or how much evidence is needed. If the circumstances of *Giberson* are used as a guide, it would seem that the court requires a near certainty. In *Giberson*, there was an incriminating document sitting next to the printer that was connected to the computer.[118] Because the document was not of high quality, the officers believed it had come from the printer.[119] The association between the document and the printer, and the printer's connection to the computer, was clear. It is difficult to imagine what different or additional circumstances could arise so as to more clearly implicate a specific computer. If the officers in *Payton* had found a printout of

---

[115] *Payton*, 573 F.3d at 863.
[116] *Id.* at 864.
[117] *Id.* at 863.
[118] United States v. Giberson, 527 F.3d 882, 884 (9th Cir. 2008).
[119] *Id.*

a pay/owe sheet in the same bedroom as the computer, but did not find the document on or near a printer, it is unclear whether the discovery of the document would have risen to the "circumstances indicating a likelihood" standard.

Thus, *Giberson*'s and *Payton's* "would be found" standard is much stricter than the "could be found" standard for traditional containers and computers used previously by the Ninth Circuit, its sister circuits, and other courts. *Payton*, by upholding *Giberson*, puts the Ninth Circuit out of line from the rest of the circuits across the country.

1. Prior to Giberson*, Ninth Circuit Precedent Followed the "Could Be Found" Reasonableness Standard*

In *United States v. Gomez-Soto*, the Ninth Circuit stated that "it is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects *might* contain the items described in the warrant."[120] In *Gomez-Soto*, officers conducted a search for documentation pertaining to drug trafficking and seized a microcassette.[121] The court upheld the seizure, noting that microcassettes are used as a device for recording all types of information, including the type that would fall within the scope of the warrant.[122] It further noted that a warrant need not predict the form of the container in which the information may be found.[123] There is no mention of ample evidence or circumstances making it likely the microcassette contained the evidence sought. Rather, it was simply because the microcassette *could* contain the information sought that the court found the seizure reasonable.

In circumstances similar to those of *Payton*, in the Ninth Circuit's unpublished case of *United States v. Sprewell*, the officers were executing a search warrant looking for evidence of drug sales.[124] Among the items sought were " 'any talley sheets or pay and owe sheets which tend to establish any narcotics and

---

[120] United States v. Gomez-Soto, 723 F.2d 649, 654 (9th Cir. 1984) (emphasis added).

[121] *Id.* at 652-54.

[122] *Id.* at 655.

[123] *Id.*

[124] United States v. Sprewell, Nos. 89-50571, 89-50695, 1991 U.S. App. LEXIS 14094, at *1 (9th Cir. June 26, 1991) (unpublished).

dangerous drug transactions.' "[125] As in *Payton*, the officers discovered a computer during their search and seized it.[126] The court drew a comparison to its analysis in *Gomez-Soto* and stated that "a computer is 'by its very nature a device for recording information.' "[127] The court upheld the seizure and explained it was not necessary to predict with precision what form the evidence would be in for the warrant to be valid.[128] In assessing whether an item described by a warrant meets the particularity requirement, the court considered whether it was *possible* for the officer to more specifically describe the items to be seized based on his or her information at the time the warrant was issued.[129] Again, there was nothing that provided extra assurance that the officers would find what they were looking for on the computer. It was enough that the computer by its very nature *could* contain what they were looking for.[130] Therefore it was reasonable for the officers to seize it.[131]

2. Other Courts Follow the "Could Be Found" Reasonableness Standard

In the Tenth Circuit case of *United States v. Carey*, officers were given written consent to search the premises for evidence of drug sales, and in the course of their search they came upon and seized a personal computer.[132] The court upheld the seizure, noting that

> "in the age of modern technology and the commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take" because drug records might be found in cassettes, leases and accounts cards, or cancelled checks.[133]

The court did not create an extra requirement that the officers executing the search find some additional evidence to implicate

---

[125] *Id.* at *10 (quoting the search warrant).

[126] *Id.* at *10-11.

[127] *Id.* at *12 (quoting *Gomez-Soto*, 723 F.2d at 655).

[128] *Id.*

[129] *Id.* at *13 (quoting United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)).

[130] *Id.*

[131] *Id.* at *10-13.

[132] United States v. Carey, 172 F.3d 1268, 1270 (10th Cir. 1999).

[133] *Id.* at 1275 n.7 (quoting United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986)).

the computer.

The Colorado Supreme Court determined that the "container rationale is equally applicable to nontraditional, technological 'containers' that are reasonably likely to hold information in less tangible forms."[134] Under this reasoning, the court upheld the seizure of five laptop computers during a search for "materials that provided instructions or examples concerning the production or use of any firearms, ammunitions, and explosive or incendiary devices or parts, as well as materials showing an intent to do physical harm or physical damage against any person or building."[135] The court found the computers were "likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material,' of a type enumerated in the warrant."[136]

Like the Ninth Circuit in *Gomez-Soto*, the Colorado Supreme Court noted that a warrant cannot always predict the form in which evidence will come.[137] The court determined that the laptops were reasonably likely to serve as containers for the writings listed in the warrant.[138] As a part of its reasonableness analysis, the court took note that the laptops "were not found in a packaged state or in any way suggesting that they could not have been used for the purposes for which they were designed," thereby making them fair game.[139]

In *Commonwealth v. McDermott*, the Massachusetts Supreme Court likewise upheld a warrantless seizure of a computer on the ground that the computer was similar to a closed container and was capable of holding documents that were sought under the search warrant.[140] Among the items sought by the officers there were documents "reflecting the possession, custody, or control of the premises; documents reflecting the purchase of, or license to carry, firearms and ammunition; documents reflecting the employment, salary, and garnishment of wages of the defendant. . . ."[141]

The California Court of Appeal for the Fourth District also upheld a seizure of a laptop computer during a search for stolen

---

[134] People v. Gall, 30 P.3d 145, 153 (Colo. 2001).
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] *Gall*, 30 P.3d at 153-54.
[139] *Id.* at 154.
[140] Commonwealth v. McDermott, 864 N.E. 471, 484 (Mass. 2007).
[141] *Id.* at 483.

goods.[142] The warrant included the authority to seize any items "tending to show dominion and control of the location," and listed a number of items in which this evidence could be found.[143] The defendant argued that the laptop was not one of the enumerated items and therefore should not have been seized.[144] The court upheld the seizure and concluded that the officers "could not be expected to divine in advance of their entry the precise nature of such evidence – whether mail, bills, checks, invoices, other documents, or keys."[145] The court further stated that it would be "patently unreasonable" for the officers to be expected to know the exact locations of such evidence.[146]

3. Payton's *"Circumstances Indicating a Likelihood" Standard Is Impractical and Creates a Loophole That Undermines Privacy*

In *Payton*, the court held the search of the computer and its subsequent seizure was unreasonable because there was no evidence to implicate the computer, even though the computer would be a logical place to find spreadsheets and other documents enumerated in the warrant.[147] The trouble with this holding is that it requires officers to have advance knowledge of the form and location in which evidence may be found (e.g., that the evidence will be electronic in nature and will be found in a computer). However, the Fourth Amendment does not require a list of the items to be searched (e.g., a safe, file cabinet, computer). Since an officer does not need to make such a showing on the original warrant, it makes little sense to create a stricter standard once a previously unknown computer is discovered.

As noted above, courts in other jurisdictions have found this requirement to be unreasonable.[148] The likely result of such a condition is that computers will be listed on a warrant if it is likely that the items sought could be found on a computer, regardless of

---

[142] People v. Balint, 41 Cal. Rptr. 3d 211, 218 (Cal. Ct. App. 2006).

[143] *Id.*

[144] *Id*. at 216.

[145] *Id.* at 217 (quoting People v. Rogers, 232 Cal. Rptr. 294, 298 (Cal. Ct. App. 1986)).

[146] *Balint*, 138 Cal. App. 4th at 208 (quoting People v. Rogers, 232 Cal. Rptr. 294, 298 (Cal. Ct. App. 1986)).

[147] United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).

[148] *See* United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999); People v. Gall, 30 P.3d 145, 153 (Colo. 2001); Commonwealth v. McDermott, 864 N.E. 471, 484 (Mass. 2007); *Balint*, 41 Cal. Rptr. 3d at 218.

any advance knowledge as to their presence in order for officers to preserve the option of a computer search should a computer be found. This in turn incentivizes an end run around the Ninth Circuit's rule that, absent listing the computer in the warrant, evidence must be found implicating a particular computer in order to render the seizure and search reasonable.[149]

C. COMPUTERS ARE NOT TRADITIONAL CONTAINERS AND SHOULD REQUIRE DIFFERENT SEARCH PROTOCOLS AND A WARRANT

Due to the vast amount of information a computer can hold, a search for a few documents can easily turn into a general search in the absence of judicial supervision.[150] The Ninth Circuit expressed such a concern if it was to uphold the search of Payton's computer under a traditional container theory, because "[s]uch a ruling would eliminate any incentive for officers to seek explicit judicial authorization for searches of computers."[151]

Since a search of a computer is fundamentally different from a search of any other type of container,[152] the better approach is to have a search protocol specific to computers. This section outlines the differences between a computer and a traditional container, such as the vastly superior amount of information a computer can hold, the mechanism by which a computer holds information, and the physical limitations of a computer. Next, this section discusses briefly how courts dealt with new technologies before the advent of computers. Finally, the section concludes by discussing the concerns outlined in *Payton*.

1. Differences Between a Computer and a Traditional Container

The impulse to analogize a computer to a traditional container is natural. A computer is an object that contains things, just as any traditional container does. However, this is where the similarity between a computer and a traditional container ends. While the contents of an open container are visible to the naked eye, a computer contains much more. In fact, it is the inherent opaqueness of a computer's digital contents, and the privacy that

---

[149] *Payton*, 573 F.3d at 863-64.
[150] *Id.* at 864.
[151] *Id.*
[152] *Payton*, 573 F.3d at 863-64.

it allows the user, that is both its damning quality (for those conducting searches) and its allure (for just about everyone else).

The first distinction between a container and a computer is that a computer does not "hold" data in the traditional sense. Rather, it is composed of data.[153] The structure of a file cabinet is a shell with drawers, and it can contain file folders. But the essence of a computer is its files – a great many files.[154] One gigabyte[155] of storage can hold 100,000 pages of single-spaced text.[156] A new computer in early 2010 has the capacity to store upwards of eight terabytes – the equivalent of roughly 800 million pages of single-spaced text.[157] Simply put, there is no traditional "container" that can match a computer in terms of the sheer volume of information it can hold.

Another obvious difference is in how the dimensions of a traditional container inherently limit a search. An officer may look for items enumerated in the warrant only in places where they might be found and cannot look in a place smaller than the item to be seized.[158] However, the natural limitation a container imposes upon a search does not apply to a computer. The computer provides no clue as to what the bytes of information stored inside it comprise. Even if it is known that a piece of evidence can be found within the computer, an officer conducting a search of that computer is provided relatively little in the way of signposts to indicate which bytes of data to examine. For example, a folder labeled "music" may not necessarily contain music files. The search can quickly become the equivalent of looking for a needle in a digital haystack.[159]

---

[153] Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2 (2007).

[154] *Id.*

[155] Gigabytes and terabytes are units of measurement for data storage capacity or computer memory. The smallest measurable unit is a bit. There are 8 bits in a byte. A gigabyte is the approximate equivalent of one million bytes. A terabyte is the approximate equivalent of one trillion bytes. *See* Byte Converter, What's A Byte?, http://www.whatsabyte.com/P1/byteconverter.htm (last visited Mar. 29, 2010).

[156] Jason McKay, *Why Should I Use Electronic Signatures?*, Articles 3000, http://www.articles3000.com/Gadgets-and-Gizmos/13901/Why-Should-I-Use-Electronic-Signatures.html (last visited Sept. 12, 2009).

[157] *Id.*; Apple Store, Mac Pro Technical Specifications, http://www.apple.com/macpro/specs.html (last visited April 11, 2010).

[158] United States v. Ross, 456 U.S. 798, 824 (1982).

[159] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 301 (2005).

2. Other Atypical Containers

Before computers, courts had to apply search and seizure requirements to other atypical containers.[160] Items such as audiotapes and pagers have been construed as types of containers that can hold potential evidence.[161] As with a computer, one cannot tell just by looking at a videotape what is stored on the videotape.[162] The only way to find out what it contains is to play it back.[163] Consequently, the Ninth Circuit has upheld a search (i.e., a "viewing") of a cassette tape,[164] and an Illinois appellate court allowed the seizure and subsequent search of an eight-millimeter tape.[165]

Despite the similarities, there are differences between a tape and a computer. At a minimum, these types of items dictate the form of the contents. An audiocassette tape will contain an audio record. With a videotape, one is assured of finding visual images. Both of these media have inherent limitations that help narrow a search. One would not play back an audiotape to search for a video recording. A computer, however, has no such limitations. If the item can be reduced to a digital form, the computer may contain it.[166]

3. Different Search Protocols for Computers

Despite the impulse to compare a computer to a container, the Ninth Circuit has shifted away from applying traditional container search protocols to computers, due to the difficulties noted above. As previously stated, while a specific search warrant is not necessary to search a traditional container, *Payton* appears to hold that a search warrant is necessary to search a computer.[167]

The *Payton* court noted the differences between the search of a computer and a search of a container. "[S]earches of computers

---

[160] United States v. Gomez-Soto, 723 F.2d 649 (9th Cir. 1984).

[161] *Id.* (microcassette audio tape); United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990) (pager).

[162] People v. Donath, 827 N.E.2d 1001, 1013 (Ill. App. Ct. 2005).

[163] *Id.*

[164] *Gomez-Soto*, 723 F.2d at 654-55.

[165] *Donath*, 827 N.E.2d at 1013.

[166] Currently, most things can be reduced to a digital form; examples include music, videos, and photographs, as well as every type of document, including books, newspapers, and bills.

[167] United States v. Payton, 573 F.3d 859, 863-64 (9th Cir. 2009).

. . . involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers. Such considerations commonly support the need specifically to authorize the search of computers in a search warrant."[168] The court further noted that "affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests."[169] In contrast, no search warrant is required to look inside a "traditional" container if it could harbor the evidence sought.[170] Thus, a computer might best be described as a "place" to be searched, rather than a type of container, making a computer more analogous to a house.

Despite acknowledging these differences, the court recognized that computers must still be susceptible to searches. It stated in *Giberson*:

> While it is true that computers can store a large amount of material, there is no reason why officers should be permitted to search a room full of filing cabinets or even a person's library for documents listed in a warrant but should not be able to search a computer.[171]

This statement, however, was made with one caveat: in order to search a computer, a warrant must be sought.[172]

III. THE NINTH CIRCUIT'S IMPLIED BRIGHT-LINE RULE

In *Payton*, the court analyzed the question of whether a search warrant that authorized (1) a search of Payton's premises and (2) seizure of records such as "[s]ales ledgers showing narcotics transactions such as pay/owe sheets," authorized the officers to look for such records in Payton's computer.[173] The *Payton* court applied its "recent and controlling precedent" of *Giberson* and answered the question in the negative. Under the facts present in *Payton*, the warrant did not authorize a search of

---

[168] *Id.* at 862.
[169] *Id.* at 864.
[170] United States v. Gomez-Soto, 723 F.2d 649, 654 (9th Cir. 1984).
[171] United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008).
[172] *Id.* at 890-91.
[173] *Payton*, 573 F.3d at 862.

Payton's computer.[174] Whether or not it intended to do so, the *Payton* court – with its imprecise discussion of *Giberson* – appears to have created a bright-line rule: to search a computer, even for items listed on a warrant that could be contained in the computer, the officers must have a warrant authorizing the computer's search.[175]

In *Giberson*, the court indicated that it was not endorsing the proposition that a "computer is an exception to the general principle that a warrant authorizing the seizure of particular documents also authorizes the search of a container likely to contain those documents."[176] The defendant in *Giberson* had urged the court to hold that, if a computer was not listed on the warrant, it could not be seized or searched.[177] But the *Giberson* court instead held that, because there had been ample evidence near the computer to indicate that "seizable items" were stored on the computer, it was reasonable for the officers "to secure the computer and obtain a specific warrant and search it."[178]

The *Payton* court summarized *Giberson* as having examined the question of whether "computers [are] exception[s] to the general principle that a warrant authorizing the seizure of particular documents also authorizes the search of a container likely to contain those documents."[179] The *Payton* court quoted *Giberson*'s holding: "We hold that, *in this case, where there was ample evidence that the documents in the warrant could be found on Giberson's computer*, the officers did not exceed the scope of the warrant when they seized the computer."[180] The *Payton* court then interpreted the passage as holding that, under certain circumstances, computers are not an exception to the rule permitting searches of containers and, by "negative inference," where such "certain circumstances" are absent, "a search of a computer not expressly authorized by a warrant is not a reasonable search."[181] Thus, the *Payton* court suggested that it was merely applying a rule already established in *Giberson*: officers can conduct a search of a computer for seizable items that could be stored in the computer only if they possess a warrant

---

[174] *Id.* at 862-63.
[175] *Id.* at 863-64.
[176] *Giberson*, 572 F.3d at 887-88.
[177] *Id.* at 886.
[178] *Id.* at 889.
[179] *Payton*, 573 F.3d at 862-63.
[180] *Id.* at 863 (quoting *Giberson*, 572 F.3d at 887) (emphasis in original).
[181] *Id.*

authorizing a search of the computer, except in circumstances where – as in *Giberson* – there is evidence indicating that the seizable items are in the computer.[182]

The *Payton* court's application of *Giberson* was flawed in two critical respects. First, the court blurs the distinction between seizing a computer and searching it. Second, in its analysis, the court glosses over the critical fact that the officers in *Giberson* obtained a subsequent warrant before conducting their search of the computer. The *Giberson* court had approved the officers' two-step process of "securing" the computer and then obtaining a *subsequent warrant* that specifically authorized its search.[183] The holding of *Payton*, and a proper reading of the *Giberson* case, leads to one conclusion: In order to search a computer for seizable items that may be found on the computer, a warrant, either the initial one or a subsequent one, is required.[184]

This conclusion is further supported by the court's repeated expression of concerns about computer searches conducted without a warrant and the need for judicial oversight.[185] The court noted that

> the nature of computers makes such searches so intrusive that affidavits seeking warrants for the search of computers often include a limiting search protocol, and judges issuing warrants may place conditions on the manner and extent of such searches, to protect privacy and other important constitutional interests.[186]

The court further stated that it was "important to preserve the option of imposing such conditions when they are deemed warranted by judicial officers authorizing the search of computers."[187] Finally, the court pointed to the officers' actions in *Giberson* and noted that the "searching officers . . . stop[ped] and [sought] an explicit warrant when they encounter[ed] a computer that they [had] reason to believe should be searched."[188]

While the Ninth Circuit rejected defendant Giberson's bright-line proposition that a computer can never be searched if it is not

---

[182] *Id.*
[183] *Id.*
[184] *Giberson*, 572 F.3d at 889; *Payton*, 573 F.3d at 863.
[185] *Payton*, 573 F.3d at 864.
[186] *Id.*
[187] *Id.*
[188] *Id.*

listed on *the original* warrant,[189] in *Payton*, it suggested that a computer cannot be searched without *a* warrant.[190] So, while other containers found during a warrant-based search may be searched under authority of the warrant, the same does not hold true for a computer. Thus in *Payton*, the Ninth Circuit appeared to do precisely what it said it would not do in *Giberson*: create a bright-line rule that a warrant is necessary for a search of a computer.

IV. TOWARD A PRACTICAL STANDARD OF REASONABLENESS IN COMPUTER SEARCHES

In practice, the apparent bright-line rule in *Payton* will likely not serve its purpose of protecting searches of computers. Officers will include computers on all future search warrants if any of the items they seek could reasonably be found on a computer. By doing so, they will preserve the option of a search without the need to present ample evidence in support of such a search but in the process will obliterate any pretense of computer privacy under the Fourth Amendment. A more practical standard of reasonableness in computer searches and warrants is needed. This Part analyzes why a seizure is often necessary before a search and concludes with a proposed guideline for future computer searches.

A. WHY A SEIZURE IS ADVISABLE BEFORE A SEARCH

The Ninth Circuit drew a distinction between the officer's actions in *Payton* and the officer's actions in *Giberson*.[191] In *Payton*, the officer searched first and seized second; whereas in *Giberson*, the officer seized first, then sought a warrant and searched second.[192] The Supreme Court has recognized the less-intrusive nature of a seizure of property, noting that, while "[a] seizure affects a person's possessory interest; a search affects a person's privacy interest."[193] The Ninth Circuit echoed this observation and acknowledged that, while "[a] seizure of a computer to await a second warrant is nevertheless a Fourth

[189] *Giberson*, 572 F.3d at 887.
[190] *Payton*, 573 F.3d at 864.
[191] *Id.* at 863.
[192] *Id.*
[193] Segura v. United States, 468 U.S. 796, 806 (1984).

Amendment seizure, . . . it is far less intrusive than a search."[194] This distinction recognizes the vast amount of information a computer can hold and the possible constitutional rights that may be trampled if the search is conducted without judicial supervision.[195] The Supreme Court has noted that, while property may be temporarily seized without a warrant, no further action will be allowed without a warrant.[196] A neutral, detached magistrate will first have to determine if there is sufficient probable cause to carry out the search of the seized property.[197]

Of course, the mandate to seize first and search second is contrary to the usual protocol of a search and seizure. Officers are allowed to seize only those items specifically authorized by the warrant.[198] The warrant must name both the specific place to be searched and the particular items to be seized.[199] Computers, however, pose a significant problem in this area because the documents to be seized, which may be in the form of electronic files, are often intermingled with scores of other files.[200] Without a search-limiting protocol in place, a search of a computer's files can quickly devolve into an impermissible and unconstitutional general search.[201]

Arguably, the absence of a search-limiting protocol is what the court was most concerned with in *Payton*.[202] The officer found the computer in Payton's bedroom, moved the mouse, deactivated the screen saver, and then clicked on the first file he saw.[203] While it is true that some of the items in the warrant could be found in the computer, there were no set limitations guiding his search. Searching a computer without established parameters is tantamount to going into a house and opening drawers indiscriminately. The Fourth Amendment is designed to prevent precisely that kind of arbitrary government search.

A computer search can require a level of technical expertise beyond that of the executing officers and can take hours to

---

[194] *Payton*, 573 F.3d at 863.

[195] *Id.* at 864.

[196] *Segura*, 468 U.S. at 806.

[197] *Id.* at 807.

[198] Maryland. v. Garrison, 480 U.S. 79, 84 (1987).

[199] *Id.*

[200] United States v. Giberson, 572 F.3d 882, 888 (9th Cir. 2008) (quoting United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001)).

[201] United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).

[202] *Id.*

[203] *Id.* at 860.

complete.[204] This is due to the possibility that the data sought "may be mislabeled, encrypted, stored in hidden directories, or embedded in 'slack space' that a simple file listing will ignore."[205] As a result, requiring officers to search through computer files on the premises in order to seize only those files listed on the warrant has been recognized as unreasonable.[206] A lengthy on-site computer search can also be overly intrusive to the premises occupants.[207] These considerations in turn have made it necessary for officers to make a wholesale seizure of the computer in order to search it at a different time and location and under the guidance of a new warrant.[208] This exemplifies how the Fourth Amendment's reasonableness requirement has demanded flexibility to adapt to the challenges of new technologies. Many courts have responded by adopting a new Fourth Amendment rule: "A valid warrant entitles investigators to seize computers and search them off-site at a later date."[209]

B. A PROPOSED GUIDELINE FOR SEIZING AND SECURING A COMPUTER

The main concern expressed by the Ninth Circuit in *Payton* is the need to protect privacy interests that are easily violated in computer searches not subject to judicial supervision.[210] If a computer is discovered in the course of a search, and it is reasonable to believe that the evidence sought could be found on the computer, the computer should be seized, and a second warrant to govern the search of the computer should be

---

[204] UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE MANUAL 77 (Sept. 2009), *available at* www.cybercrime.gov/ssmanual/02ssma.pdf.

[205] *Id.* at 76. "Slack space" is the unused space at the end of a file in a disk cluster. PC Magazine Encyclopedia, Definition of: Slack Space, http://www.pcmag.com/encyclopedia_term/0,2542,t=slack+space&i=56995,00.asp (last visited Apr. 24, 2010). A hidden directory is invisible when looking at the directory listing in which it exists. The Linux Information Project, *Hidden File Definition*, http://www.linfo.org/hidden_file.html (last visited Apr. 24, 2010). Encryption is typically used for file security. It is the process in which words are changed into an unreadable code. Answers.com, http://www.answers.com/topic/encryption (last visited Apr. 24, 2010).

[206] United States v. Henson, 848 F.2d 1374, 1383-84 (6th Cir. 1988).

[207] United States v. Schandl, 947 F.2d 462, 465-66 (11th Cir. 1991).

[208] *Id.*

[209] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 315 (2005).

[210] United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).

obtained.[211]

There are practical considerations in implementing such a procedure. As was the case in *Payton*, computers are frequently left "on" and in screen-saver mode or in standby or sleep mode.[212] In order to seize a computer and protect the computer's data (and physical components in the computer itself), the computer must be properly powered down. Failing to do so could jeopardize unsaved work in open applications and possibly the entire hard drive.[213] In order to preserve the integrity of the computer, Fourth Amendment protections, and the administration of justice, officers should follow this proposed set of guidelines in order to establish a clear and consistent protocol for computer seizures:

Proposed Computer Seizure Protocol

1. Note the circumstances that lead the officer to believe the computer may contain the evidence sought on the warrant. Examples of such circumstances include whether the evidence sought is easily reduced to digital form[214] and whether there is anything prohibiting the computer from working in its normal capacity.[215]

2. Note whether the computer is powered off, in screen-saver mode, or in standby or sleep mode. By recording the status of the computer, the officer can justify moving the mouse as would be necessary to properly power down the computer.[216]

---

[211] Recommended computer search protocols and guidelines are beyond the scope of this Note.

[212] When a computer is in standby or sleep mode, it is still "on," but the screen appears dark because the computer is using less electricity. A screen saver is activated on most computers when a computer is not in use after a specified period of time (as set by the user). The purpose of a screen saver is to prevent phosphor burn-in on the computer screen – something that was of concern with older cathode-ray-tube screens but less so now with LCD screens.

[213] A computer typically comes with a resource guidebook warning against improperly shutting down the computer. For example, the Toshiba Resource Guide, for the Satellite A80/A85 Series Laptop Computer, notes that "[t]urning off the computer while it is reading from or writing to a disk may damage the disk, the drive, or both." It also states that "[i]f the network you are using goes down and you must restart your computer to reconnect, or if your battery runs out of charge while you are working, you will lose all work since you last saved."

[214] Examples are documents that can be created with computer software, scanned, or downloaded off the Internet, or any photos, video or voice recordings.

[215] This was one of the considerations applied by the Colorado Supreme Court in *People v. Gall*, 30 P.3d 145, 154 (Colo. 2004).

[216] "Power down" is equivalent to "turn off."

a. If the computer is in standby or sleep mode, move the mouse or press the return key to reactivate the screen. Record what is on the screen. This would ensure a complete and accurate record of what was done and what was seen in the course of seizing the computer.

b. If the computer is in screen-saver mode, note what is on the screen saver. Move the mouse and de-activate the screen saver. Note again what is on the screen.

3. Save any open documents. This needs to be done to protect against the possible loss of any data.

4. Close all open applications. This will ensure against possible corruption to the computer hard drive and its applications.

5. Power down the computer properly.

By recording the steps taken in seizing the computer and making a note of all that was done and seen, a complete record of what happened to the computer will be available for both the police and the magistrate.[217] The officer should then prepare a new affidavit seeking a search warrant from the magistrate. The affidavit should state the reasons why a search of the computer is necessary, outline the steps that were taken to preserve the computer and its contents during the seizure, and describe the search protocol that will be used to protect privacy interests. This equivalent of chain-of-custody documentation would serve the government's interest in preserving evidence while protecting the individual's right of privacy in his or her computer.

V. CONCLUSION

In *Payton*, the Ninth Circuit properly reversed the district court's denial of a motion to suppress the evidence obtained by way of a computer search not listed in a warrant. However, the court based its reasoning on an impractical standard of reasonableness that it first enunciated in *Giberson*. In order to search a computer not listed on a warrant, the court stated there must be circumstances indicating a likelihood that the items to be

[217] Images revealed on the computer screen, as the steps are taken to power off the computer, may then become subject to the plain-view doctrine. A discussion of the plain-view doctrine is beyond the scope of this Note.

seized are contained in the computer.[218] This standard means that it is not enough that the items sought could reasonably be found on the computer. This creates a significantly stricter standard than that employed for traditional containers.

In *Payton* and *Giberson*, the Ninth Circuit appears to have done precisely what it said it would not do: create a bright-line rule for computers. The court distinguished computers from traditional containers and applied to computers a heightened standard of Fourth Amendment reasonableness.[219] The court further implied that, in order to search a computer, it is necessary to procure a search warrant.[220] By obtaining a warrant, the court reasoned that constitutional privacy interests could be protected.[221] Since the circumstances in *Payton* failed to meet the heightened reasonableness standard and the officer did not obtain a search warrant before searching the computer, the court arrived at the correct result: suppression of the evidence. But the court's new standard has the unfortunate effect of creating hurdles for police officers seeking to conduct a computer search. To get around the heightened reasonableness standard that requires demonstrating circumstances that show evidence would be found on a particular computer, officers will request authorization to search a computer in every case where evidence could be reduced to a digital form. This will undermine the very privacy interests that the *Payton* court sought to protect.

In computer search cases, when officers need to seize a computer for a subsequent search, they should follow the *Proposed Computer Seizure Protocol* in order to ensure that privacy interests are protected and that the integrity of the computer remains intact. This will have the benefit of enhancing the government's ability to properly prosecute crimes while at the same time preserving citizens' privacy rights under the Fourth Amendment. That is a result that surely would satisfy the *Payton* court.

---

[218] United States v. Payton, 573 F.3d 859, 863 (9th Cir. 2009) (quoting United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008)).

[219] *Id*. at 864.

[220] *Id.* at 863.

[221] *Id.* at 864.

SUSAN A. RADOS[*]

[*] J.D. Candidate, May 2011, Golden Gate University School of Law, San Francisco, Cal.; M.A. and B.A. Radio and Television, San Francisco State University, San Francisco, Cal. My thanks to the members of the *Golden Gate University Law Review* Editorial Board for their helpful suggestions and guidance during the writing process. And a special thank you to my husband, Richard, without whose love and support this Note would never have been finished.