Department of Homeland Security
Federal Law Enforcement Training Center
Legal Training Division

February 2010

The Federal Law Enforcement -Informer-

MONTHLY LEGAL RESOURCE AND COMMENTARY FOR FEDERAL LAW ENFORCEMENT OFFICERS AND AGENTS

Welcome to this installment of *The Federal Law Enforcement Informer (The Informer)*. The Legal Division of the Federal Law Enforcement Training Center is dedicated to providing federal law enforcement officers with quality, useful and timely Supreme Court and Circuit Court reviews, interesting developments in the law, and legal articles written to clarify or highlight various issues. The views expressed in these articles are the opinions of the author and do not necessarily reflect the views of the Federal Law Enforcement Training Center. *The Informer* is researched and written by members of the Legal Division. All comments, suggestions, or questions regarding *The Informer* can be directed to the Editor at (912) 267-2179 or FLETC-LegalTrainingDivision@dhs.gov. You can join *The Informer* Mailing List, have *The Informer* delivered directly to you via e-mail, and view copies of the current and past editions and articles in *The Quarterly Review* and *The Informer* by visiting the Legal Division web page at: http://www.fletc.gov/legal.

This edition of *The Informer* may be cited as "2 INFORMER 10".
(The first number is the month and the last number is the year.)

Join The Informer E-mail Subscription List

It's easy! Click HERE to subscribe, change your e-mail address, or unsubscribe.

THIS IS A SECURE SERVICE. No one but the FLETC Legal Division will have access to your address, and you will receive mailings from no one except the FLETC Legal Division.

Announcing
the
Police Legal Advisors Training Program
(PLATP)

The course is designed for currently employed attorneys for state and local law enforcement agencies and departments. Managers of those agencies and departments are invited on a space available basis.

April 19-23, 2010
Naval Station Mayport, FL

Click HERE

for a detailed description of the program and registration form.

2009 Legal Division
Handbook
Reference Book

Now Available for Purchase at the
GPO On-Line Bookstore

Click HERE to Order

Click HERE to download the

Supplement to the 2009 Legal Division Handbook

CASE SUMMARIES

CIRCUIT COURTS OF APPEALS

2nd CIRCUIT

Burg v. Gosselin, 2010 U.S. App. LEXIS 289, January 07, 2010

Looking at this issue for the first time, the court decides:

The issuance of a pre-arraignment, non-felony summons requiring a later court appearance, without further restrictions, does not constitute a Fourth Amendment seizure. This summons does no more than require appearance in court on a single occasion, and operates to effectuate due process.

The 1st, 3rd, 6th, 7th, 8th, 9th, 10th, and 11th circuits agree (cites omitted)**.**

Editor's Note: In a previous 2nd Circuit case (cite omitted), a defendant accused of offenses that included two felonies was released post-arraignment, but was ordered not to leave the State of New York pending resolution of the charges against him, thereby restricting his constitutional right to travel outside of the state. He was obligated to appear in court in connection with those charges whenever his attendance was required, culminating in some eight appearances during the year in which his criminal proceeding was pending. The Court ruled that these restrictions imposed on the defendant constituted a "seizure" within the meaning of the Fourth Amendment.

Click **HERE** for the court's opinion.

******

4th CIRCUIT

U.S. v. Day, 2010 U.S. App. LEXIS 429, January 08, 2010

The Fourth Amendment does not provide protection against searches by private individuals acting in a private capacity. Similarly, the sole concern of the Fifth Amendment, on which Miranda was based, is governmental coercion. The defendant bears the burden of proving that a private individual acted as a government agent.

There are two primary factors to be considered: (1) whether the government knew of and acquiesced in the private individual's challenged conduct; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation.

With regard to the first factor, there must be some evidence of government participation in or affirmative encouragement of the private search. Passive acceptance by the government is not enough. Virginia's extensive armed security guard regulatory scheme simply

empowers security guards to make an arrest. This mere governmental authorization for an arrest, in the absence of more active participation or encouragement, is insufficient to implicate the Fourth and Fifth Amendments.

With regard to the second factor, even if the sole or paramount intent of the security officers had been to assist law enforcement (in deterring crime), such an intent would not transform a private action into a public action absent a sufficient showing of government knowledge and acquiescence under the first factor of the agency test.

Under the "public function" test typically utilized for assessing a private party's susceptibility to a civil rights suit under 42 U.S.C. § 1983, private security guards endowed by law with plenary police powers such that they are *de facto* police officers, may qualify as state actors. Security guards who are authorized to arrest only for offenses committed in their presence do not have plenary police powers and are not *de facto* police officers.

Click **HERE** for the court's opinion.

******

U.S. v. Williams, 2010 U.S. App. LEXIS 1327, January 21, 2010

The sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents.

The search warrant authorized a search of defendant's computers and digital media for evidence relating to the designated Virginia crimes of making threats and computer harassment. To conduct that search, the warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization. To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance. Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality.

Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied.

○○○○○○

The warrant also authorized the police to search for things like disks and "thumbnail drives," which, the evidence showed, could be as small as a dime, and which could very easily have been stored in the lockbox where the machine gun and silencer were found. A thorough search of the lockbox would therefore have required the detective to move the gun and silencer, even if only within the confines of the lockbox. And before moving the gun, the detective was entitled to pick it up and determine whether it was loaded, for his own safety. Because it was during the course of a legitimate safety inspection that the

incriminating character of the machine gun and silencer became "immediately apparent," the warrantless seizure of them was justified by the plain-view exception.

Click **HERE** for the court's opinion.

******

U.S. v. Abdelshafi, 2010 U.S. App. LEXIS 1568, January 25, 2010

To establish a violation of § 1028A(a)(1), the Government must prove the defendant (1) knowingly transferred, possessed, or used, (2) without lawful authority, (3) a means of identification of another person, (4) during and in relation to a predicate felony offense.

Nothing in the plain language of the statute requires that the means of identification at issue must have been stolen. For sure, stealing and then using another person's identification would fall within the meaning of "without lawful authority." However, there are other ways someone could possess or use another person's identification, yet not have lawful authority to do so. Defendant may have come into lawful possession, initially, of Medicaid patients' identifying information and had lawful authority to use that information for proper billing purposes, but he did not have lawful authority to use Medicaid patients' identifying information to submit fraudulent billing claims.

The application of § 1028A(a)(1) is not limited to cases in which an individual's identity has been misrepresented. Such an interpretation is not supported by the plain text of the statute.

Click **HERE** for the court's opinion.

******

7th CIRCUIT

U.S. v. Kilgore, 2010 U.S. App. LEXIS 377, January 08, 2010

In the case of a felon in possession of a firearm, the justification (necessity) defense only applies to the individual who in the heat of a dangerous moment disarms someone else, thereby possessing a gun briefly in order to prevent injury to himself. It is available when the felon, not being engaged in criminal activity, does nothing more than grab a gun with which he or another is being threatened (the other might be the possessor of the gun, threatening suicide). The defense is a rare one and is unavailable in a setting where no ongoing emergency exists or where legal alternatives to possession are available.

Click **HERE** for the court's opinion.

******

U.S. v. Mann, 2010 U.S. App. LEXIS 1264**,** January 20, 2010

Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents. Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.

The search warrant authorized a search for "images of women in locker rooms and other private places." Given the nature of the search and the fact that images of women in locker rooms could be virtually anywhere on the computers, using software known as "forensic tool kit" ("FTK") to catalogue the images on the computer into a viewable format did not, without more, exceed the scope of the warrant.

But, the "FTK" software also employed a filter known as "KFF (Known File Filter) Alert." The "KFF Alert" flags those files identifiable from a library of known files previously submitted by law enforcement—most of which are images of child pornography. The "KFF Alert" flagged four files. Once those files had been flagged, the detective knew (or should have known) that files in a data base of known child pornography images would be outside the scope of the warrant. The detective exceeded the scope of the warrant by opening the four flagged "KFF Alert" files.

Click **HERE** for the court's opinion.

Editor's Note: The Court rejected the rule set out by the 9th Circuit in U.S. v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009), that directs magistrate judges to insist that the government waive reliance on the plain view doctrine. Instead, the court counsels officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described.

(On November 4, 2009, the 9th Circuit entered an order asking the parties in U.S. v. Comprehensive Drug Testing, Inc. to brief the question of whether the case should be reheard by the full en banc court (comprised of *all* active judges as opposed to the 11 ordinarily selected randomly for standard en banc review).)

******

U.S. v. Pappas, 2010 U.S. App. LEXIS 1271, January 21, 2010

Obtaining a warrant is prima facie evidence of good faith on the part of the officer. Consulting with the prosecutor prior to applying for a search warrant provides additional significant evidence of that officer's objective good faith.

An officer can reasonably believe that the number of email messages containing child pornography (11 over two months in this case) sent to defendant, and the risk inherent in sending even one image of child pornography to anyone other than a willful recipient, is

sufficient to establish probable cause for the crime of knowing possession of child pornography.

○○○○○○

A warrant application that includes boilerplate language concerning the practices of collectors of child pornography must lay a foundation which shows that the person subject to the search is a member of the class. However, there is no magic "profile" of child pornography "collectors" that must be attested to in a search warrant affidavit. In fact, the moniker "collector" merely recognizes that experts in the field have found that because child pornography is difficult to come by, those receiving the material often keep the images for years. There is nothing especially unique about individuals who are "collectors" of child pornography; rather, it is the nature of child pornography, i.e., its illegality and the difficulty procuring it, that causes recipients to become "collectors." Where evidence indicates that an individual has uploaded or possessed multiple pieces of child pornography, there is enough of a connection to the "collector" profile to justify including the child pornography collector boilerplate in a search warrant affidavit.

Click **HERE** for the court's opinion.

******

9th CIRCUIT

Elliot-Park v. Manglona, 2010 U.S. App. LEXIS 723, January 12, 2010

While an officer's discretion in deciding whom to arrest is certainly broad, it cannot be exercised in a racially discriminatory fashion. There is no right to state protection against madmen or criminals, but there is a constitutional right (equal protection) to have police services administered in a nondiscriminatory manner—a right that is violated when a state actor denies such protection to disfavored persons. A complete withdrawal of police protective services based on race or ethnicity violates equal protection. Diminished police services also don't satisfy the government's obligation to provide services on a non-discriminatory basis. The government may not racially discriminate in the administration of *any* of its services.

The right to non-discriminatory administration of protective services is clearly established. The very purpose of 42 U.S.C § 1983 was to provide a federal right of action against states that refused to enforce their laws when the victim was black.

Click **HERE** for the court's opinion.

******

U.S. v. Pineda-Moreno, 2010 U.S. App. LEXIS 625, January 11, 2010

Agents installed mobile tracking devices on the underside of defendant's Jeep on seven different occasions. Each device was about the size of a bar of soap and had a magnet affixed to its side, allowing it to be attached to the underside of a car. On five of these

occasions, the vehicle was located in a public place. On the other two occasions, between 4:00 and 5:00 a.m., agents attached the device while the Jeep was parked in defendant's driveway a few feet away from his trailer. The driveway leading up to the trailer was open, and there was no fence, gate, or "No Trespassing" sign.

The undercarriage is part of the car's exterior, and as such, is not afforded a reasonable expectation of privacy.

Even assuming the Jeep was on the curtilage, it was parked in his driveway, which is only a semiprivate area. In order to establish a reasonable expectation of privacy in his driveway, defendant must detail the special features of the driveway itself (i.e. enclosures, barriers, lack of visibility from the street) or the nature of activities performed upon it. Because defendant did not take steps to exclude passersby from his driveway, he cannot claim a reasonable expectation of privacy in it, regardless of whether a portion of it was located within the curtilage of his home. The time of day agents entered the driveway is immaterial.

Click **HERE** for the court's opinion.

******

U.S. v. Palos-Marquez, 2010 U.S. App. LEXIS 1112, January 19, 2010

The in-person nature of a tip, even from an unidentified informant, gives it substantial indicia of reliability for two reasons. First, an in-person informant risks losing anonymity and being held accountable for a false tip. Second, when a tip is made in-person, an officer can observe the informant's demeanor and determine whether the informant seems credible enough to justify immediate police action without further questioning.

○○○○○○

In the context of border patrol stops, relevant facts for reasonable suspicion include: (1) characteristics of the area; (2) proximity to the border; (3) usual patterns of traffic and time of day; (4) previous alien or drug smuggling in the area; (5) behavior of the driver, including obvious attempts to evade officers; (6) appearance or behavior of passengers; (7) model and appearance of the vehicle; and, (8) officer experience.

Click **HERE** for the court's opinion.

******