

THE FOURTH AMENDMENT, SEARCHES INCIDENT TO ARREST,
AND PERSONAL DIGITAL STORAGE DEVICES

Craig M. Jaquith
Assistant Ohio Public Defender
ACLU of Ohio Conference
July 30-31, 2010

The Fourth Amendment to the United States Constitution provides that “[t]he 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.” Generally, a law enforcement officer is prohibited from conducting a search unless he or she has “first convince[d] a neutral magistrate that there is probable cause to do so.” But U.S. Supreme Court case law has long held that “the exigencies of the situation” may sometimes make a warrantless search constitutionally permissible.

Further, the Court has held that police may, incident to a person's arrest, search the arrestee's person and the area within the arrestee's “immediate control” without a warrant. The Court determined that warrantless searches are permissible incident to a lawful arrest 1) to prevent the arrestee from gaining access to a weapon, which might be used to assault an officer, and 2) to prevent the arrestee from destroying or concealing evidence of his crime.

Under the “search incident to arrest” doctrine, police may search the entire body and immediate grabbing space of an arrestee, including the contents of all containers, even if they lack probable cause to believe that such a search will produce evidence of the offense of arrest. In light of this well-established exception to the warrant requirement, and the widespread and ever-increasing use of portable electronic data storage devices such as cell phones, smartphones, tablet computers, and laptop computers, it quickly becomes apparent that rules must be established regarding when and how such devices may be searched. The purpose of this brief overview is to assess, with respect to such searches, where things stand now, and where they may be headed.

Although there is some case law regarding the search of digital storage devices found on the person of an arrestee, there is not yet a great number of such cases, and there is little agreement among those cases in terms of an overarching analytical framework. The earliest cases dealt with digital pagers, commonly used by drug dealers in the 1990s as a mode by which they could be contacted by potential buyers. The courts that reviewed the constitutionality of warrantless searches of simple pagers did not hesitate to determine that forcing the government to obtain warrants would create the risk of destruction of evidence, due to new numbers “pushing out” old ones. Further, because the devices stored only phone numbers, the privacy interests at stake were minimal—there was no concern about the police “cyber-rummaging” through a pager, because it cannot store contact information, text messages, photos, etc.

In more recent years, as the cases have turned from searches of pagers to searches of cell phones of varying degrees of sophistication, there has been some recognition that the devices are different. But there has been one aspect of the cell phone cases that court decisions tend to agree on, and it seems fair to say that this area of agreement would likely surprise the average citizen: the vast majority of the courts analogize a modern cell phone to a simple “closed container,” and thus permit searches of phones without a warrant and without probable cause to believe it contains evidence relevant to the crime of arrest.

The key case involving the search of a “closed container” found on the person of an arrestee arose from the search of a crumpled cigarette pack that happened to contain heroin. Quite simply, and not very surprisingly, the U.S. Supreme Court has determined that if an arrestee has a cigarette pack, a pill bottle, a purse, or any other container capable of holding evidence, contraband, or a weapon, that container may be searched at the time of arrest, or immediately upon booking, without first obtaining a warrant.

Rather remarkably, it seems that of the courts that have been presented with the issue to date, only the Ohio Supreme Court has declined to view a cell phone that is sophisticated enough to hold text messages, photos, voice memos, etc., as a device comparable to a simple closed container. All other courts have either explicitly or implicitly embraced the “closed container” analogy, and use that body of law to deem warrantless cell phone searches to be permissible. This is in spite of plain language from the U.S. Supreme Court that a closed container is defined as a “any object capable of holding another object,” and the inarguable fact that digital storage devices do not contain

“objects.” The handful of cases outside of Ohio that have required suppression of evidence found pursuant to a warrantless cell phone search have been based on the fact that the search took place too long after the arrest, rather than the seemingly obvious fact that a digital storage device is not a simple closed container.

The vast majority of cell phone-search cases involve scenarios where the police have probable cause to believe that the device contains incriminating evidence—and obviously it did contain such evidence, or else the offender would not be bringing an appeal challenging the legality of the search—thus it is easy to adopt a no-harm, no-foul attitude. After all, the Fourth Amendment by its terms only protects against “unreasonable” searches and seizures. But there is immense potential for police abuse if the courts continue to employ the closed-container approach to justify such warrantless searches.

That potential for abuse stems from the fact that closed-container searches have historically been permissible even if the police lacked probable cause to believe that they would find evidence related to the arrest. Thus, it is easy to think of a hypothetical, such as the disorderly-conduct arrest of Professor Henry Louis Gates, Jr., in which the police would gain access to an individual’s call logs, contact lists, text messages, personal photos, etc., regardless of whether those matters had anything to do with the crime for which the individual was being arrested. And, by logical extension, if a cell phone is a closed container, why should a laptop computer not also be deemed to be a closed container, subject to an extensive, warrantless search by the government? Further, there would seemingly be nothing preventing the police from opening a “dossier” for any such arrestee, filing away for future use the information gleaned in the “closed container” search.

Because the judicial use of the closed-container approach in cases involving digital storage devices does not seem to adequately foresee such scenarios, let alone attempt to prevent them, and because digital devices are becoming vastly more sophisticated and powerful every year, a different analytical approach is necessary. One possible approach would be the one that Ohio has taken: no warrantless search can occur unless the police are motivated by exigent circumstances. Because other courts around the nation have not yet been inclined to take this approach, and because it is a very defense-friendly rule, it seems unlikely that this will ever become the majority approach. Further, with the increased use of smartphones, which generally seem to have the capability of having data

erased by remote manipulation, it will be increasingly easy for the police to plausibly argue “exigent circumstances” as a legitimate basis for conducting a warrantless search.

Although not as clear or as protective a rule as Ohio’s “no search without a warrant” rule, it seems that one approach that is likely to come into greater acceptance in the future is to allow searches of such devices upon a suspect’s arrest, but only where probable cause exists that the device contains evidence relevant to the offense of arrest. Further, under this approach, the scope of the search would be limited to areas of the device, for example call logs, where the evidence is thought to exist. This approach would require the creation of a new rule of law, because it does not readily flow from any existing legal doctrine. But because the police and the courts are having to deal with an entirely new category of devices, it should not be surprising that a new rule of law may be required to create a meaningful framework for such cases.

One theoretical advantage to this approach is that mistaken-identity cases could be identified at the arrest stage—if the suspect’s device does not contain the information the police are looking for, they may conclude that they have arrested the wrong person. But an obvious downside to this limited-search approach is that there would be no way to ensure that the police do not access other areas of the device that contain personal information unrelated to the offense of arrest. If the police come upon incriminating evidence that they would not have viewed if they had done a properly limited search, then presumably such evidence of a different crime could be suppressed. But there would ultimately be no way of ensuring that the police were not obtaining and retaining personal information that never would have been available to the police if the individual had not been arrested.

In sum, how to apply the Fourth Amendment in cases involving the search of a portable digital storage devices seized during a lawful arrest is a question that is certain to be asked with increasing frequency in the coming years. While “bright line” rules have great advantages in terms of providing clear guidance both to law enforcement personnel and to citizens, there is sufficient variability between such devices, and technology is evolving so rapidly, that it is arguable that establishing a rule or set of rules today would be premature. But it seems likely that some variation of the approach suggested above—it is permissible for the police, with probable cause, to conduct immediate, limited, warrantless searches for evidence—will become the rule of law ultimately crafted to address this recurring and increasingly important issue.