Search Incident to Arrest of Personal Electronic Devices

By Richard Gissel, Defender Investigator, Juvenile Division

It seems new personal electronic devices are introduced daily. Pagers, laptop computers, personal digital assistants, cell phones, and thumb flash drives are but a few of the personal electronic devices people carry with them everyday. These devices can contain huge amounts of information that people might believe to be safe and secure. Yet, in this post 911 era, many people are unaware that their personal information is open to examination if they are arrested. Changing technologies present tough questions about how these devices fit within the current framework of court cases and laws.

The United States Supreme Court held in *United States v. Robinson*[1] that police can search a person and items within that person's control incident to an arrest. The Court found that officer safety and preservation of evidence interests prevail over personal privacy rights, making such searches reasonable under the Fourth Amendment. The guidelines for a search incident to arrest seem simple to follow on its surface, but new electronic technologies complicate the matter. Lower courts have relied upon *Robinson* to guide them when determining if the police actions were reasonable retrieving information within devices carried by those arrested.

Time limits are even less troublesome when items to be search are immediately associated with the accused. In *United States v. Edwards*,[2] the Supreme Court reasoned that as long as the administrative process incident to the arrest had not been competed, a search of effects seized from the accused is still incident to the arrest and, therefore, permissible. Yet, questions remain about the extent to which these principles extend to personal electronic devices and the digital evidence contained within.

Digital Evidence

Digital evidence is simply information in a digital format such as e-mails, digital photographs, digital videos, word processing documents, and instant message histories. Its use has increased in recent years as the courts have applied the *Federal Rules of Evidence* to define digital evidence in the same manner as more traditional documents, but courts have also noted important differences. The courts have found that digital evidence is difficult to destroy, easily changed and copied, and more readily available. For these reasons, some courts treat digital evidence differently for purposes of hearsay, authentication, the best evidence rule, and privilege. Still, as the courts have become comfortable with digital formats they have ruled "computer data compilations… should be treated as any other records."[3]

Searching Personal Electronic Devices

Most challenges to digital evidence center around authenticity questions such as "Was the data altered?", "Was the program that generated the data reliable?", and "Who is the author of the data?" But, a far more important question to consider: "Was the data legally obtained?"

Laptop Computers

A person may carry several personal electronic devices on them at any one time and if arrested these devices can become the subject of a warrantless search. Yet, the courts have looked at the right-to-privacy issue about data on computers and found there is a reasonable expectation of privacy concerning digital files stored on a laptop computer.[4] Still, it is important to note that (1) a person may lose his right to privacy if he allows a third-party access to that data; and (2) the right to privacy does not extend to searches conducted by private parties not acting for the government. For example,

in *United States v. Hall*,[5] the defendant had taken his laptop to be repaired and the technician found child pornography on it. Authorities got a search warrant based on information given by the technician. The court ruled, "Seizure of an entire computer was justified when the warrant narrowly described the child pornography files sought, since agents would not, under the terms of the warrant, be free to rummage through the defendant's property."

Recently, there has been a shift away from a focus on privacy to one of security. Generally, a computer in a private home cannot be searched without a warrant, but at the border it is a different story. Customs agents have the power to read, seize, and store all the information that can be retrieved from laptops of travelers entering the United States. The Ninth Circuit Court of Appeals held that forensic analysis of a laptop by U.S. Immigration and Customs Enforcement is permissible without probable cause or a warrant. The court ruled, "under the border search exception, the government may conduct routine searches of persons entering the United States without probable cause, reasonable suspicion, or a warrant."[6] However, when the question arises about a search incident to arrest of a laptop, the courts look toward rulings regarding other personal electronic devices like cell phones.

Cell Phones

Today most people carry with them a cell phone which is regularly found on defendants or within their immediate control if arrested. In the *United States v. Finley,* a cell phone was taken from the defendant during a search incident to a lawful arrest. With a codefendant they were taken to the codefendant's home where authorities were carrying out a search warrant. During the search of the home, the memory of the cell phone found on the defendant was searched and several text messages related to drug trafficking were found. This information was later used to convict the defendant. On appeal the court found the defendant did have an expectation of privacy regarding the contents of the cell phone, but the search was within the scope of a search incident to arrest. Further, the court ruled the fact the cell phone was not searched right away after the custodial arrest did not change the validity of the search.[7]

In *United States v. Mercado-Nava,* the defendant was arrested after a narcotics dog alerted on his truck and drugs were found. The arresting officer found a cell phone on the defendant and downloaded its entire memory at the time. The court upheld the search of the defendant's cell phone under the preserve evidence prong of the search incident to arrest exception. The court ruled that the "need to preserve evidence is underscored where evidence may be lost due to the dynamic nature of the information stored on…cell phones."[8] Under these decisions, the data on a cell phone is encompassed by the search incident to arrest exception.

Pagers

Until cell phones became popular, pagers fulfilled the major role as the common personal communications device. A pager is a simple telecommunications device that receives a short message consisting of a few digits, such as a phone number that the user can call. Although pagers have become obsolete, they are still used in niche markets like emergency services. Pagers are also still preferred by some who like their simplicity and privacy. Although pagers are not common, the courts have ruled that information contained on them is open to search incident to arrest. For example, in *United States v. Chan*, the court denied the defendant's motion to suppress information gained from his pager as a result of a lawful search incident to his arrest. The court found the search of the pager was conducted contemporaneous to the arrest and was a lawful search under the Fourth Amendment.[9]

Flash Cards

IPods, digital cameras, GPS, and even wristwatches are but a few personal electronic devices that use flash cards. A flash card, sometimes called a memory card, offers high record abilities, extensive

data and power-free storage, and a rugged environment to keep data safe. The courts have not yet ruled on the legality of search incident to arrest of flash cards which might be carried by a defendant unattached from a personal electronic device. Still, it would stand to reason the courts would follow the same logic when called on to decide the validity of a flash card search incident to arrest.

Areas to Consider

One area to consider when forming a possible defense strategy might be based on statutory protections granted some wire and electronic communications at both the federal and state levels. These statutory provisions restrict the intentional intercepting of some forms of wire or electronic communication unless approved by a court order. Of course each case will have to be analyzed on its own merits and facts to decide if these provisions apply.

Another developing legal area regarding the search of personal digital devises is Fifth Amendment protections. Government agencies have stressed the need to collect electronic information in the name of public safety, especially after September 11th. For example, travelers entering the United States routinely have the information on their laptops copied even if that information is proprietary. There is also an expectation that travelers not only show how their digital devises work but also surrender personal passwords as well. But this requirement is under scrutiny in the courts. The United State District Court of Vermont recently ruled that a defendant did not have to reveal his personal password to the government. To do so would violate the defendant's Fifth Amendment right against self-incrimination. The court stated: "The government can force a person to give up the key to a safe because a key is physical, not in a person's mind. But a person cannot be compelled to give up a safe combination because that would 'convey the contents of one's mind,' which is a 'testimonial' act protected by the Fifth Amendment." The court's ruling is on appeal.[10]

Summary

Be prepared for prosecutors to argue that if the police can search a person incident to arrest and seize any evidence found, then personal electronic devices should be treated the same. There are important distinctions, however, that defense counsel can emphasize. For example, the information on a flash card can take days to examine and will still be available in full if simply impounded and not searched. Further, under the Fourth Amendment the search must be reasonable. Improved privacy protections, like encryption and passwords, moreover, may be key to establishing another tier of protection under the Fifth Amendment.

References

1. *United States v. Robinson,* (414 U.S. 218 1973)
2. *United States v. Edwards*, 415 U.S. 800 (1974)
3. *United States v. Vela*, 673 F.2d 86, 90 (5th Cir. 1982).
4. *United States v. Barth,* 26 F. Supp. 2d 929, 936-7 (W.D. Tex. 1998)
5. *United States v. Hall*, 142 F. 3d 988 (7th Cir, 1998)
6. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985)
7. *United States v. Finley*, 2007 U.S. App. LEXIS 1806 (5th Cir. 2007)
8. *United States v. Mercado-Nava*, 2007 WL 1098203 (District of Kansas 2007),
9. *United States v. Chan,* 830 F.Supp. 531 (N.D. Cal., 1993).
10. In Child Porn Case, a Digital Dilemma -http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663.html