WARRANTLESS SEARCHES & SEIZURES: CONSENT, SEARCH INCIDENT TO ARREST & PROBABLE CAUSE-BASED VEHICLE SEARCHES

Professor Thomas K. Clancy

OBJECTIVE:

In this session, you will learn how to apply several traditional doctrines of Fourth Amendment satisfaction to digital devices, including: (1) consent, (2) search incident to arrest, (3) inventory searches and (4) probable cause-based searches of vehicles.

REQUIRED READING:

1. Thomas K. Clancy, Fourth Amendment Satisfaction: Traditional Exceptions to Warrant Requirements (Apr. 2012) [NCJRL PowerPoint].................................................................1
Fourth Amendment satisfaction: traditional exceptions to warrant requirement

National Center For Justice And The Rule Of Law
University of Mississippi School of Law

Thomas K. Clancy
Director

www.NCJRL.org

materials

1. powerpoints
2. Chapter 7 (consent)
   Chapter 8 (warrantless searches; excerpt)

Clancy, Cyber Crime and Digital Evidence - Materials and Cases
(Lexis Nexis 12/2011)

consent searches: three considerations

#1 must be voluntary

* question of fact

* based on totality of circumstances
#2 scope of consent

person may limit scope of search

objective TEST: “what would the typical reasonable person have understood by the exchange between the officer and the suspect?”

scope:
- typically defined by its expressed object
- extends to entire area in which object of search may be found and not limited by possibility that separate acts of entry or opening may be required

---

   - Can I look at your cell phone?
   - response: “Go ahead”

2. U.S. v. Lemmons, 282 F.3d 920 (7th Cir. 2002):
   - Is there anything on the computer that we should be aware of?
   - response: “take a look”

Where can police look?

---

#3 third party consent

Two types

1. Actual Authority:
   - person has common authority over or other sufficient relationship to object to be searched

2. Apparent Authority:
   - reasonable reliance by police on consent of person who seems authorized to consent based on facts known to officer at time consent was given
U.S. v. Luken, 560 F.3d 741 (8th Cir. 2009)

"I ... give law enforcement the permission to seize and view my Gateway computer."

discussed w/ police
  - they believed he had CP
  - nature of computer s, could recover deleted files

Can police forensically examine computer?


• illegal cloned cell phone -- calls billed to another #

  Q: can we s/ vehicle for "guns, drugs, money, or contraband?"

• search of phone -- removed batteries, short circuit test revealed serial # did not match

  exceed scope of consent?

Joint Users and Passwords

Joint Users

general rule: joint user can consent to search

Password-Protected Files

creator "affirmatively" intends to exclude
  joint user & others from files

--- does NOT assume risk joint user would permit S/
3rd party consents to s/ computer — police use software that copies ("mirrors")
--- does not detect passwords – later examine files

U.S. v. Buckner, 473 F.3d 551 (4th Cir. 2007)
wife had apparent authority
note: cannot use technology to intentionally avoid discovery of password / encryption

U.S. v. Andrus, 483 F.3d 711 (10th Cir. 2007)
parent had apparent authority
note: no factual basis for claim of high incidence of password use
-- if so, would put in Q use of software that overrides such use

Are computers containers or something "Special?"

view #1: Data are Documents / Container Analogy
view #2: "Special Approach" to S/ of data on computers

two views: apply to all digital devices

Can police search Cell Phone incident to arrest?

☐ YES:
are containers - based on "binding" SCT precedent
    People v. Diaz, 244 P.3d 501 (Cal. 2011)
application of per se rule to digital evidence containers

U.S. v. Finley, 477 F.3d 250 (5th Cir. 2007)
  - upholding search of cell phone recovered from arrestee's pocket

U.S. v. Ortiz, 84 F.3d 977 (7th Cir. 1996)
  - upholding retrieval of information from pager

case law rejecting SIA application to cell phones

☐ NO: are not containers and persons have “higher level of privacy” in info “they contain”
  State v. Smith, 920 N.E.2d 949 (Ohio 2009)

  - U.S. v. Wall IV
    - unreported: cell phones used during U/C drug sting
      - search occurred at police station
    - "searching through information stored on a cell phone is analogous to a search of a sealed letter, which requires a warrant"

Searches of digital devices located in vehicles without a warrant

  some traditional methods:
  1. Search incident to arrest
  2. inventory
  3. probable cause
Vehicle “black boxes”

- Event data recorders
- Sensing and diagnostic modules
- Data loggers

seat belts, brakes used, weather, speed, location ....

Digital devices

- Infiniti G35
  - 9.5 GB hard drive

- Cadillac CTS
  - 40 GB hard drive

fax machine

http://www.prodesks.com/

check out the video

2009 dodge ram with wi fi
search incident arrest

traditional doctrine

- rationale: 1. officer safety
  2. recover evidence that could be destroyed

- exigency: prior to Robinson v. United States, 414 U.S. 218 (1973)

  often viewed as exception to warrant requirement -- intimated exigent circumstances rationale and, perhaps, need to justify each case

Robinson changed this: per se rule

categorical approach of Robinson

only showing: legal custodial arrest

"It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a "reasonable" search . . .
**permissible scope of SIA**

1. **person:** "unqualified authority"
   
   *Robinson*

2. **reach and grasp area:** area w/ in "immediate control"
   
   *Chimel*

3. **vehicles:** entire passenger compartment
   
   *Belton*

---

**Scope:** vehicle searches incident to arrest


incident to arrest of auto occupant, police may search entire passenger compartment of car, including any open or closed containers, but not the trunk

“**Container**

Any object capable of holding another object. "It thus includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like.”

---

**Arizona v. Gant:**

new approach for vehicles!!

**Gant’s two holdings:**

1. NO vehicle search incident to occupant’s arrest after arrestee secured and cannot access interior of vehicle

   **or**

2. circumstances unique to automobile context justify search when reason to believe that evidence of offense of arrest might be in vehicle
essential rationale:

1. **protect privacy interests** -

   *Belton* searches authorizes of every purse, briefcase, or other container within passenger compartment

   "A rule that gives police the power to conduct such a search whenever an individual is caught committing a traffic offense... creates a serious and recurring threat to the privacy of countless individuals."

holding #1 explained

*can SIA* "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search"

fn4:

"...it will be the rare case in which an officer is unable to fully effectuate an arrest so that a real possibility of access to the arrestee's vehicle remains"

holding #2 explained

circumstances unique to automobile context justify S/IA when reasonable to believe that evidence of offense of arrest might be in vehicle

std: "reasonable basis"
application to digital evidence containers

People v. Díaz, 244 P.3d 501 (Cal. 2011)

SI A as to persons: delayed searches


- seemed to abandon contemporaneous limit for searches of person
- permitted s/ of arrestee's clothing at jail 10 hours after arrest

“It is . . . plain that searches and seizures that could be made on the spot at the time of the arrest may legally be conducted later when the accused arrives at the place of detention.”

distinguishing between objects closely associated w/ person and other effects?

U.S. v. Chadwick, 433 U.S. 1 (1977) dicta:

[W]arrantless searches of luggage or other property seized at the time of an arrest cannot be justified as incident to that arrest either if the “search is remote in time or place from the arrest,” or no exigency exists. Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control . . . a search of that property is no longer an incident of the arrest.

- FN distinguishing Edwards: “Unlike searches of the person, searches of possessions within an arrestee's immediate control cannot be justified by any reduced expectations of privacy caused by the arrest.”
A dubious jurisprudence of containers

Subsequent lower court case law:

immediately associated

- wallets
- purses
- backpacks

not closely associated

- luggage

Diaz -- cell phone (90 minutes after arrest)

---

applying SIA principles

---

the stakes: iPhone in driver's pocket

1. activates touch screen to view phone's contents
2. clicks on internet browser icon
3. clicks on toolbar to find bookmarks link
4. finds suspicious-looking bookmark labeled “porn pictures”
5. clicks on bookmark to bring up webpage
6. webpage contains series of icons including “members” button; clicks image
7. brings up “members” page - has saved account number / password already entered
8. clicks “submit” button which utilizes saved acct info / password to bring up content of website
9. sees pictures and message function; account owner has new messages
10. brings up new messages, which detail incriminating conversation about exchanging pictures of underage children
inventory searches

current doctrine:

- may conduct inventory search of contents of autos and personal effects lawfully in police custody
- must be pursuant to routine administrative policy, cannot be solely to look for evidence of criminal conduct
- purpose is to protect owner's property, police against false claims for stolen or lost property, and police & others from potential danger

examples:


permissibility of inventory searches involves two inquiries:

(1) was original seizure of item reasonable?

(2) was inventory properly conducted pursuant to routine administrative policy?

inventory searches

arguably cannot search cell phones / computers / other digital devices that are lawfully seized and subject to inventory

reason:

no reason to retrieve data to protect it

BUT:

what if the policy permits examination of data?


**Case Law Rejecting Inventory Application to Cell Phones**

- *People v. Nottoli*, 130 Cal. Rptr. 3d 884 (Cal. App. 2011)
  
  *rejects: don’t need to know contents to safeguard*

  
  "no need to document the phone numbers, photos, text messages, or other data stored in the memory of a cell phone to properly inventory because the threat of theft concerns the cell phone itself, not the electronic information stored on it."

**Probable Cause Based Vehicle Searches**

- inquiry unchanged:
  
  - do police have PC to search vehicle?
  - is digital data with in scope of search for which there is PC?
  
  - (Ex) *People v. Xinos*, 121 Cal. Rptr. 3d 496 (Cal. App. 2011)
  
  - no PC to search black box in prosecution for vehicular manslaughter while driving DUI when download occurred long after accident and no reason to believe DEF had been speeding
Chapter 7

CONSENT SEARCHES; COMPELLING DISCLOSURE OF PASSWORDS

This chapter addresses the validity of consent to search computers — a Fourth Amendment issue — and addresses compelling a suspect to disclose his password or encryption key — a Fifth Amendment issue.

§ 7.1 CONSENT — IN GENERAL

The principles regulating the permissibility of a search or seizure based on a claim of consent do not change in the context of computer and other digital evidence searches. However, computers and digital evidence searches present several challenges to the application of those principles.

Consent to search is a question of fact and is determined based on the totality of the circumstances. The ultimate question turns on the voluntary nature of the consent. A person may “delimit as he chooses the scope of the search to which he consents.” The government, in performing a search, cannot exceed the scope of the consent given. This is an objective inquiry: “what would the typical reasonable person have understood by the exchange between the officer and the suspect?” Moreover, the scope of a consensual search is generally defined by its expressed object. This is to say that consent “extends to the entire area in which the object

---

1 See, e.g., United States v. Mabe, 330 F. Supp. 2d 1234 (D. Utah 2004) (rejecting assertion that defendant consented to search of computer after police falsely stated that they had search warrant); People v. Yuruckso, 746 N.Y.S.2d 33, 34-35 (N.Y. App. Div. 2002) (consent to search home computer valid, based on defendant’s maturity, education, and other factors, even though police stated that, if he did not consent, they would obtain a search warrant and seize his work computer).


3 See, e.g., Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). Voluntariness — meaning the lack of coercion by the government agents — must be established. However, the consent need not be an informed one, which is to say that the person giving the consent need not know that he or she has the right to refuse, which is the essential holding of Schneckloth.


6 Id. See also United States v. Raney, 342 F.3d 551, 558 (7th Cir. 2003) (seizure of “homemade” adult pornography within scope of consent to search for “materials [that] are evidence in the nature of child abuse, child erotica, or child exploitation” as it showed ability and intent to manufacture pornography depicting himself in sexual acts); United States v. Turner, 169 F.3d 84, 88-89 (1st Cir. 1999) (scope of defendant’s permission to search apartment in connection with intruder’s assault on neighbor exceeded when police accessed files on his computer because the police request would have been reasonably
of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search."

For example, when a graduate student in computer science agreed to allow agents to search his entire home and to take his computer back to the FBI office for further examination, it was held that the student "would have realized that the examination of his computer would be more than superficial when the agents explained that they did not have the skills nor the time to perform the examination in his home." Moreover, according to the court, "a graduate student in computer science would clearly understand the technological resources of the FBI and its ability to thoroughly examine his computer." Given the lack of limitations put on the search by the student, his cooperation, and his expertise, the court believed it was reasonable for the agents to conclude that they had unlimited access to the computer.

§ 7.2 CONSENT — SCOPE ISSUES

PEOPLE v. ROBERT S. PRINZING
907 N.E.2d 87 (Ill. Ct. App. 2009)

JUSTICE BOWMAN delivered the opinion of the court.

Robert S. Prinzing was convicted of possessing child pornography. He argues that, even if his consent was valid, the evidence should have been suppressed because the police exceeded the scope of his consent. We agree that the police exceeded the scope of the consent, and we reverse and remand.

The trial court held an evidentiary hearing on defendant’s motion to suppress. Detective Smith testified as follows. He was employed with the Kane County sheriff’s department and assigned to computer crimes and forensics. On October 29, 2003, he spoke with Ronald Wolfick, a special agent with Immigration and Customs Enforcement. Wolfick provided Detective Smith with information regarding online credit card purchases of child pornography and provided the credit card number used, which belonged to defendant. Detective Smith obtained a subpoena and contacted the bank that issued the credit card. The bank told Detective Smith that a fraudulent charge had been reported around the time that the card was used to purchase child pornography. The bank relayed that a new account number had been issued. On May 25, 2004, Detective Smith, along with
Detective Grimes went to defendant’s residence. Detective Smith identified himself and stated that he was investigating fraud involving defendant’s credit card. Detective Smith inquired “as to his card usage, the geographical area in which he might have used it, also if it was ever out of his control and through the course of the conversation trying to determine if he had lost control of that card where someone else could have acquired his credit card numbers.” Defendant retrieved his credit card and gave it to Detective Smith. Detective Smith recognized the number as the one that had been used to purchase child pornography. Defendant told Detective Smith that he owned the credit card and maintained exclusive control over the card. Defendant stated that he used the card in the local area, when he went on trips, and occasionally for Internet purchases. Detective Smith asked defendant whether there had been any fraud reported on his credit card. Defendant stated that there had been an incident of fraud, his money was refunded, and he was issued a replacement card.

Detective Smith told defendant that if he used the card on the Internet, there was opportunity for others to steal his information. Detective Smith asked defendant if he still possessed the computer that he used to make Internet purchases. If there was any evidence of his system being compromised by unsafe Internet Web sites or a virus, it would likely be on the computer used to make Internet purchases. Defendant denied noticing any suspicious activity on his credit card. Defendant worked for Comcast and was very knowledgeable about computers, impressing Detective Smith. Defendant denied having any suspicion that the security on his computer had been compromised. Detective Smith testified that a virus could infect a computer when a person received a spam e-mail or visited a particular Web site embedded with the virus. He had an investigatory tool that allowed him to check for such viruses.

Detective Smith asked defendant if he could search his computer by using a special program, with the intent of trying to determine how his credit card information might have been stolen. Defendant consented. According to Detective Smith, he initially used a noninvasive tool to perform a “preview,” which prevents any changes from happening to the computer when the system is turned off and on. The “preview” allows detectives to view the hard drive but prevents them from making any changes to any of its files. Normally, after the “preview” program, Detective Smith would use a program called “Image scan.” The image scan looks for images related to Web pages to get a history of pages that the user has visited. The program brings up thumbnail images from Web pages. Depending upon what is found, he then would use a tool that would look for viruses or any key stroke loggers, which capture key strokes and send the information to a remote location. Detective Smith began the search of defendant’s computer by using the image scan program. He was looking for thumbnails with the Visa logo, not for child pornography. Detective Smith testified that he did not inform defendant that he believed that his credit card information had been used to access child pornography Web sites, because “at this point [he] didn’t feel that [defendant] still had been — was the offender. [Detective Smith] was curious as to how his information could have been compromised.” He was concerned that defendant’s credit card may have been compromised not once, but twice. Detective Smith explained that “when you visit a web site, if you go to make a purchase, you will see
a Visa logo. That will be captured. Whatever the merchandise is being offered on that particular web page, it will have graphics that will show that.” A Visa credit card number will not be captured. Detective Smith would have to click on the image to get to the vendor’s Web site.

Detective Smith found several images that he suspected were child pornography. He found the images within 10 to 15 minutes after he began the scan. He denied that he was specifically looking for child pornography. Rather, he was looking for information related to defendant’s credit card. He considered his investigation up to this point to be related to credit card fraud because there was evidence of only a few attempts to access the pornographic Web sites, whereas other investigations involved numerous attempts.

On cross-examination, Detective Smith admitted [inter alia] that he was specifically assigned to review cases that involved Internet child pornography [and that he was investigating the defendant for possession of child pornography].

Defendant testified. Around 5 p.m. on May 25, 2004, two detectives arrived at defendant’s home. They told him that they were investigating a fraud case, which he thought was unusual considering that he did not have any complaints regarding any type of fraud. The detectives questioned him for approximately 10 or 15 minutes regarding his credit cards and credit card numbers. They asked if he had a particular credit card but did not inform him how they had acquired his credit card information. He produced all of the credit cards in his wallet. He told Detective Smith that he had a disputed charge at one time but that it had been resolved and he had been issued a new card. He thought that perhaps the credit card number that the detectives had was his old card number. His disputed charge took place sometime in June 2003. He had another disputed charge in August 2003, but a new card was not issued then. The detectives asked about his card usage and whether he was the sole user. They then asked to view his computer to check for viruses that could have stolen his credit card information. Defendant stated that “Detective Smith asked to view [the] computer to look for viruses, you know, signs that [a] hacker had been in [defendant’s] computer, Trojan horses, worms, anything that might possibly capture key strokes that [he] was typing in to get [his] credit card information.” He initially told the detectives that he did not feel it was necessary, because he had several firewalls in place and felt secure in his computer usage. Detective Smith insisted that it would be better for him to check defendant’s computer because his programs were better than anything that is available commercially. After the third request, defendant agreed to allow Detective Smith to check his computer.

Detective Smith then produced a USB port cable and a couple of disks that he retrieved from his briefcase. He inserted a disk into defendant’s computer, rebooted it, and then began looking at images that were on the computer. Defendant stated that it appeared that the program was creating files of pictures, because Detective Smith went to “a directory and [was] opening up different files, and every time he opened one up, it was populating with pictures from [the] computer.” Defendant never saw any images with credit card logos; he saw only images that he had downloaded from the Internet or from his digital camera. Defendant was employed by Comcast, and he regularly checked systems for...
viruses. The programs he used to check for viruses never brought up images but only executable files. Viruses are not embedded in images but are executable programs. He thought it was odd that Detective Smith was looking only at pictures but defendant did not say anything. After about 15 to 20 minutes, Detective Smith stated that he was done looking at the computer and that he found an image that he felt was child pornography.

In its ruling, the trial court stated that it believed that Detective Smith's investigation of defendant initially related to child pornography, morphed into a credit card fraud investigation when he discovered that there was a disputed charge on defendant's card, and then, after he discovered child pornography on defendant's computer, morphed back to a child pornography investigation.

[After first determining] that defendant's consent was voluntary, we now examine whether the police exceeded the scope of the consent. In evaluating the scope of a defendant's consent, the court considers what a reasonable person would have understood by the exchange between the officer and the defendant. "[T]he parameters of a search are usually defined by the purpose of the search."

In this case, principles of law and technology collide. The court in *People v. Berry*, 731 N.E.2d 853 (Ill. App. 2000), addressed the scope of consent with respect to electronic devices, specifically a cellular phone. The *Berry* court stated that the lack of knowledge of what the officer is searching for does not change the effect of a "general" consent. If a consent to search is entirely open-ended, a reasonable person would have no cause to believe that the search will be limited in some way, and the consent would include consent to search the memory of electronic devices. The *Berry* court then considered the totality of the circumstances, which involved a detective asking to look at the defendant's cell phone and the defendant responding "'go right ahead.'" The officer, after receiving the defendant's response, opened the phone and retrieved the phone number of the phone by pressing a button. The defendant knew when the detective asked to search the phone that he was investigating a murder and that he was trying to determine whether the defendant owned the phone, and the defendant placed no explicit limitations on the scope of the search, either when he gave his general consent or while the officer examined the phone. Therefore, the court determined that, based on the totality of the circumstances, the detective did not exceed the scope of the defendant's general consent to search his phone when the detective activated the phone and retrieved the phone number.

Federal courts have also considered the scope of electronic device searches. In *United States v. Lemmons*, 282 F.3d 920, 925 (7th Cir. 2002), the court determined based on the totality of the circumstances that a police search did not exceed the defendant's general consent to search his computer. The police originally obtained consent to search for video recordings of the defendant's neighbor's bedroom. Once inside, the defendant showed police a sexually explicit photograph of his 17-year-old daughter. The police then asked whether there was anything on the defendant's computer that they should be aware of, and the defendant turned the computer on and invited the officers to look. The officers then opened images saved on the computer that were pornographic images of children. The court stated that the officers' search of the computer may have been illegal if the defendant had stuck to...
his original consent to search for a camera or recording device, or if he had limited his consent to search his computer to images of his neighbor, depending on the defendant’s labeling system or other variables. Because the defendant did not limit the consent to search his computer, the police did not exceed the scope by searching random images.

In *United States v. Brooks*, 427 F.3d 1246, 1249 (10th Cir. 2005), the police requested to search the defendant’s computer for child pornography by means of a “pre-search” disk. The police told the defendant that the pre-search disk would bring up all the images on the computer in a thumbnail format so that they could check for images of child pornography. Defendant asked if it would search text files and he was told that it would not. For some reason, the disk was not operating on the defendant’s computer, so the officers performed a manual search of images. The defendant complained that the police exceeded the scope of his consent because they did not use the pre-search disk as he was told. The court disagreed, finding that the method in which the search was performed was irrelevant because the defendant knew that images would be searched and the officers searched only images and nothing more.

We find this case distinguishable from *Berry, Lemmons*, and *Brooks* because those cases dealt with general consents to search. Here, Detective Smith, by his own words, limited the scope of the intended computer search. Detective Smith specifically requested to search defendant’s computer for viruses or key-logging programs to find out if defendant’s credit card number had been stolen. The exchange between Detective Smith and defendant involved only an investigation of credit card fraud and the potential that someone had stolen defendant’s credit card number by way of a computer virus. By Detective Smith’s own description of the scanning programs that he normally used, the image scan disk searched images and Web site pages on the computer. According to Detective Smith’s testimony, if an image came up with a Visa logo, Detective Smith could click on it and he would be brought to the Web page of the vendor. He did not testify that the vendor Web page would indicate whether defendant’s credit card number was compromised. In fact, according to defendant, who worked for Comcast, no image would lead Detective Smith to discover a virus that could steal defendant’s credit card number, as viruses and key-logging programs are executable files and not embedded in any image. Defendant consented to a search only for viruses, not images. Thus, we find that Detective Smith’s search exceeded the scope of defendant’s consent.

**Justice O’Malley, dissenting:**

The . . . question is whether the police exceeded the scope of defendant’s consent by viewing the images on his computer.

The principle to be drawn is not that an officer may have no purpose for a consent search ulterior to his stated purpose, but instead that a description of the purpose of a search can serve as an indicator of the scope of the contemplated search and thus can help define the scope of the consent. The restriction on the search comes not from the stated purpose of the search, but from what the a reasonable person would have understood the extent of the consent to be — i.e., what areas a reasonable person would have understood police had been granted authority to
search. Courts say that the scope of a search generally is defined by its purpose because the stated purpose of a proposed search will often be the only explanation of the scope of the proposed search: the scope of a consent to a “search for drugs” without further explanation will be understood in those terms. Thus, police who describe a proposed automobile search by telling the suspect that they wish to search for liquor will have limited the scope of their search to places where liquor could be found, but any other contraband found in the course of that search may still lawfully be seized. Or, police who tell a suspect that they intend to search for weapons when they actually expect to find drugs may still seize drugs during their search, because “such a statement on the part of [law enforcement] could [not] affect the validity of [the suspect’s] consent, the area to be searched being identical in either event.”

It becomes very important to determine precisely how Smith and defendant described the requested search before defendant assented. The testimony is ambiguous on this point. It is true, as the majority and the parties note, that Smith told defendant that his purpose in searching the computer was to look for malware. However, the testimony does not include any description of how Smith described to defendant the process by which he would search the computer for malware. The majority seems to assume from this gap in the testimony that the only description given was that Smith would perform a “virus search,” and the majority therefore repeats or implies several times that the scope of the consent was limited accordingly. I disagree with the majority’s assumption.

Although the testimony does not directly state what Smith and defendant discussed prior to defendant’s consent, it does provide clues. When asked to describe how he would search defendant’s computer for malware, Smith described using an “image scan” program that boots the computer in a read-only mode and then calls up all of the images on the computer. The majority and the parties incorrectly imply that Smith testified that he examined the images themselves for signs of malware, but in his testimony Smith actually described differently the connection between the image scan and the search for malware. Smith said that he used the program to search for viruses because the program revealed the origin of each of the images, and, for those images originating from Web sites, Smith could ask defendant if he recalled visiting the sites. According to Smith, “[i]f someone [was] accessing his computer remotely unbeknownst to him, he [could] tell [Smith] then and there” that he had not visited the sites. Smith said that he focused his search on images portraying credit card logos, because such images often appear on Web pages that collect credit card numbers for purchases.

The efficacy of this “image viewing” technique as a virus search, especially when compared to the type of actual virus search Smith testified he forwent in order to do the image search, is questionable — a point with which the majority appears to agree. However, the issue here is not whether Smith pursued a search that would reveal viruses but, rather, whether he pursued a search consistent with the scope of the consent he had obtained, i.e., consistent with what a reasonable person would have understood as the scope of the consent defendant granted. Smith’s testimony contains the following passage:
“Q. And when you asked him to view his — when you asked about his computer, was that your intent to try and use those programs?
A. Yes, sir.
Q. And did you, in fact, inform the defendant of that?
A. Yes sir.”

In the absence of testimony that directly relates how Smith described the program to defendant before defendant agreed to the search, Smith’s description of the image scan program as a tool for detecting malware, convincing or not, gives us insight into the conversation referenced in his testimony.

Defendant’s actions after the image search began provide added insight into what the two men discussed before defendant granted consent. Smith testified that defendant was in the room when Smith started the image scan program, watched as Smith conducted a review of the images on the computer, and continued to talk to Smith as Smith ran the program, yet never asked Smith to stop viewing the pictures. While it is true that a defendant’s silence cannot be used to transform the original scope of the consent, it can provide an indication that the search was within the scope of the consent.

From the above, I infer that Smith discussed the image scan program with defendant before defendant granted consent, and, even if I were to conclude that Smith misled defendant as to the purpose of using the program, I would conclude that Smith’s use of the program fell within the scope of the consent.

NOTES
What is the permissible scope of a search of a computer for “viruses?” Is that a technical question? Is looking at logos within the scope of such a search?

1. Scope: Does consent to search include forensic exam?

UNITED STATES v. JONATHAN LUKEN
560 F.3d 741 (8th Cir. 2009)

MELLOY, CIRCUIT JUDGE.
An Immigration and Customs Enforcement investigation revealed that two credit card numbers believed to be Luken’s were used in 2002 and 2003 to purchase child pornography from a website in Belarus. On July 25, 2006, three law-enforcement officers visited Luken at his place of employment. One of the officers, Agent Troy Boone of the South Dakota Department of Criminal Investigation, informed Luken that the officers believed Luken’s credit card had been used to purchase child pornography. Boone told Luken that the officers wanted to speak with Luken
privately about the matter and look at his home computer. Luken agreed to speak with them at his home and drove himself to his house to meet them.

Upon arriving at Luken’s home, Luken allowed the officers to enter his house. Luken’s wife was home, so Boone offered to speak with Luken privately in Boone’s car. Luken agreed. Once inside the car, Boone informed Luken that Luken did not have to answer any questions, was not under arrest, and was free to leave. Luken nevertheless agreed to speak with Boone. Luken discussed the nature of his computer use and knowledge. He admitted to purchasing and downloading child pornography for several years. He also admitted to looking at child pornography within the previous month. He stated, however, that he believed he had no child pornography saved on his computer.

After Luken admitted to viewing child pornography, Boone asked Luken if officers could examine Luken’s computer. Boone explained the nature of computer searches to Luken and told Luken that, even if files had been deleted, police often could recover them with special software. Boone asked Luken if a police search would reveal child pornography in Luken’s deleted files. Luken stated that there might be “nature shots” on his computer, i.e., pictures of naked children not in sexually explicit positions, that he recently viewed for free. Boone then asked Luken to consent to a police search of Luken’s computer, and Boone drafted a handwritten consent agreement stating, “On 7-25-06, I, Jon Luken, give law enforcement the permission to seize & view my Gateway computer.” Luken signed and dated the agreement.

[The police seized the computer and Boone later] used forensic software to analyze it. Boone discovered approximately 200 pictures he considered child pornography.

The question before us is whether it was reasonable for Boone to consider Luken’s consent to seize and “view” his computer to include consent to perform a forensic analysis on it. We believe it was.

Before Luken consented to police seizing and viewing his computer, Luken initially had told Boone that Luken believed there was no child pornography saved on his computer. Boone, however, explained to Luken that police could recover deleted files using special software. Boone then specifically asked Luken if such a search would reveal child pornography on Luken’s computer. Luken responded that there probably would be such material on his computer and stated that police might find “nature shots” if they did such a search. At that point, Luken gave Boone permission to seize and view his computer without placing “any explicit limitation on the scope of the search.”

Given the above-described exchange, we agree with the district court that a typical reasonable person would have understood that Luken gave Boone permission to forensically examine Luken’s computer. Boone made it apparent to Luken that police intended to do more than merely turn on Luken’s computer and open his easily accessible files. Boone explained that police possessed software to recover deleted files and asked Luken specifically if such software would reveal child pornography on Luken’s computer. Luken responded by telling Boone that such a search would likely reveal some child pornography. He then gave Boone permission to seize and view the computer. In that context, a typical reasonable person would
understand the scope of the search that was about to take place. Therefore, because we affirm the district court's finding that Luken consented to the search, we hold there were no Fourth Amendment violations.

2. Cell Phones: Scope of Consent

**JERMAINE L. SMITH v. STATE**

713 N.E.2d 338 (Ind. Ct. App. 1999)

**KIRSCH, JUDGE.**

Smith appeals his conviction of theft, for using a “cloned” cellular telephone reprogrammed to have an internal electronic serial number (“ESN”) different than its external ESN. Put in the vernacular, Smith was convicted of using an illegal cellular phone which had been modified such that, when in use, the charges would be billed to someone else’s active cellular phone number.

Indiana State Police Sergeant David Henson pulled over a blue and white Oldsmobile driven by Steve Martin, in which Smith was a front seat passenger. Trooper Henson initiated the traffic stop because a computer check on the vehicle’s license plate revealed the plate was registered to a yellow Oldsmobile rather than a blue and white one. Trooper Henson approached the vehicle and asked Martin for his license and registration. Following the arrival of Troopers Troy Sunier and Patrick Spellman, Martin and Smith were asked to exit the vehicle, separated, and questioned in an effort to determine if the car was stolen. The troopers’ inquiries revealed that the car belonged to Smith, who had painted it a different color, which explained the apparently mismatched license plate.

During the course of this investigatory stop, Trooper Dean Wildauer arrived on the scene and asked Smith if he and Trooper Spellman could search the vehicle for guns, drugs, money, or illegal contraband. Smith consented to the search. While no guns, drugs, money, or illegal contraband were recovered as a result of the search, two cellular flip phones were retrieved from the front seat of Smith’s car. One phone was found on the passenger’s side of the vehicle where Smith had been sitting, and the other was found on the driver’s side where Martin had been sitting. When asked whether the cellular phone found on the passenger’s side was his, Smith stated that it was his girlfriend’s; however, he could not recall the name of her service provider.

Trooper Wildauer then took both phones back to his police vehicle where he removed the batteries and performed a short-out technique on each device. The results of this field-test revealed that the cellular phones’ internal ESNs did not match the external ESNs, indicating that the cellular phones had been illegally cloned, or reprogrammed such that, when in use, the charges would be billed to someone else’s phone number. After discovering that the phones were cloned, Trooper Wildauer called a law enforcement hotline which informed him that the internal ESN of the cellular phone Smith claimed was his girlfriend’s in fact belonged to GTE Mobilnet and was assigned to one of its legitimate service
customers, Technology Marketing Corporation. Upon further questioning, Smith admitted that he had purchased the cloned phone on the street from an acquaintance and that he knew it was a clone.

Initially, we observe that Sergeant Henson's investigatory stop of Smith's vehicle was valid and supported by reasonable suspicion. There are no such indicators here that Smith's consent was in any way induced by fraud, fear, or intimidation. Under the totality of these circumstances, we conclude that Smith's consent to search his vehicle was voluntarily given.

Having held that Smith's consent to search was not constitutionally defective, we must then determine whether the troopers exceeded the scope of his consent. The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of objective reasonableness, in other words, “what would the typical reasonable person have understood by the exchange between the officer and the suspect?” In addition, the scope of a consensual search is generally defined by its expressed object.

Here, the expressed objects of the troopers' search were guns, drugs, money, or illegal contraband. When Smith gave the troopers permission to search his car for guns, drugs, money, or illegal contraband, a reasonable person would have understood Smith's consent to include permission to search any containers inside the vehicle which might reasonably contain those specified items. A cellular phone is a container capable of hiding such items as drugs or money. Therefore, it was proper for the troopers to seize the cellular phone long enough to determine whether it was truly an operating cellular phone or merely a pretense for hiding the expressed objects of their search.

Smith's consent did not authorize the troopers to access the computer memory of his cellular phone — an objectively reasonable person assessing in context Smith's verbal exchange with the troopers would have understood that the troopers intended to search only in places where Smith could have disposed of or hidden the specific items which they were looking for, namely, guns, drugs, money or other contraband. No objective person would believe that by performing a short-out technique on a cellular phone to retrieve its electronic contents, the troopers might reasonably find the expressed object of their search. Thus, where the troopers here obtained consent to search Smith's car for guns, drugs, money, or contraband, they had to limit their activity to that which was necessary to search for such items.

§ 7.3 THIRD PARTY CONSENT

The validity of third party consent depends on whether the person giving consent has either actual authority or apparent authority to consent. In general, a third party may consent to a warrantless search when that party possesses “common authority over or other sufficient relationship to the premises or effects sought to be inspected.”

---

Common authority is . . . not to be implied from the mere property interest a third party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.\textsuperscript{11}

The issue frequently arises in the context of shared computer use. The question, as with consent generally, turns on the person’s access or control of the computer, regardless of whether the person is a spouse,\textsuperscript{12} parent,\textsuperscript{13} other family member,\textsuperscript{14} house mate,\textsuperscript{15} bailee,\textsuperscript{16} systems administrator,\textsuperscript{17} or other third party,\textsuperscript{18} such as a computer repair person.\textsuperscript{19}

1. Passwords and Encryption

The presence of password-protected files is an important consideration in assessing a third party’s authority to consent. By creating password-protected files, the creator “affirmatively” intends to exclude the joint user and others from

\textsuperscript{11} \textit{Matlock}, 415 U.S. at 171 n.7.
\textsuperscript{12} See \textit{Walsh v. State}, 512 S.E.2d 408, 411-12 (Ga. Ct. App. 1999) (defendant’s wife had authority to consent to search of computer that she purchased and was available for use by family).
\textsuperscript{13} See \textit{People v. Blair}, 748 N.E.2d 318, 324-25 (Ill. Ct. App. 2001) (father, who had no actual or apparent ownership of computer, could not validly consent to seizure of son’s computer).
\textsuperscript{14} See \textit{State v. Guthrie}, 627 N.W.2d 401 (S.D. 2001) (son-in-law possessed common authority over computer and could validly consent to its seizure when he had unconditional access and control over it).
\textsuperscript{15} See \textit{United States v. Smith}, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (housemate had authority to consent to search of defendant’s computer, to which she had joint access and which was located in common area of house; alternatively, government agents reasonably believed housemate could consent to search).
\textsuperscript{16} See \textit{United States v. James}, 353 F.3d 606, 614-15 (8th Cir. 2003) (bailee, who agreed to store disks and who had been later directed to destroy them, did not have actual or apparent authority to permit police to take and examine them).
\textsuperscript{17} A systems administrator is the person “whose job is to keep [a computer] network running smoothly, monitor security, and repair the network when problems arise.” \textit{U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 25} (3d ed. 2009). Those administrators “have ‘root level’ access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems.” \textit{Id.} Whether a systems administrator “may voluntarily consent to disclose information from or regarding a user's account varies based on whether the network belongs to a communications service provider, a private business, or a government entity.” \textit{Id.}
\textsuperscript{18} See \textit{United States v. Meek}, 366 F.3d 705, 711 (9th Cir. 2004) (“Like private phone conversations, either party to a chat room exchange has the power to surrender each other’s privacy interest to a third party.”).
\textsuperscript{19} United States v. Barth, 26 F. Supp. 2d 929, 938 (W.D. Tex. 1998) (computer repair person did not have actual authority to consent to search of customer’s hard drive, having “possession of the unit for the limited purpose of repair” and did not have apparent authority when police knew his status).
the files. Under such circumstances, it has been reasoned, it cannot be said that the person has assumed the risk that the joint user would permit others to search the files. On the other hand, the lack of passwords to protect files has been held to defeat a claim that the defendant had exclusive control of a computer and that his housemate did not have authority to consent to search.

UNITED STATES v. RAY ANDRUS
483 F.3d 711 (10th Cir. 2007)

MURPHY, Circuit Judge.

Federal authorities first became interested in Ray Andrus during an investigation of Regpay, a third-party billing and credit card aggregating company that provided subscribers with access to websites containing child pornography. The investigation of Regpay led to an investigation of Regpay subscribers. One of the subscribers providing personal information and a credit card number to Regpay was an individual identifying himself as “Ray Andrus” at “3208 W. 81st Terr., Leawood, KS.” The Andrus Regpay subscription was used to access a pornographic website called www.sunshineboys.com. Record checks with the drivers license bureau and post office indicated Ray Andrus, Bailey Andrus, and a third man, Richard Andrus, all used the West 81st Terrace address. The credit card number provided to Regpay was determined to belong to Ray Andrus. The email address provided to Regpay, “bandrus@kc.rr.com,” was determined to be associated with Dr. Bailey Andrus.

Eight months into the investigation, agents believed they did not have enough information to obtain a search warrant for the Andrus residence. They, therefore, attempted to gather more information by doing a “knock and talk” interview with the hope of being able to conduct a consent search. ICE Special Agent Cheatham and Leawood Police Detective Woollen arrived at the Andrus house at approximately 8:45 a.m. on August 27, 2004. ICE Special Agent Kanatzar, a forensic computer expert, accompanied Cheatham and Woollen to the residence, but waited outside in his car for Cheatham’s authorization to enter the premises.

Dr. Andrus, age ninety-one, answered the door in his pajamas. Dr. Andrus invited the officers into the residence and, according to the testimony of Cheatham and Woollen, the three sat in Dr. Andrus’ living room, where the officers learned that Ray Andrus lived in the center bedroom in the residence. In response to the officers’ questions, Dr. Andrus indicated Ray Andrus did not pay rent and lived in the home to help care for his aging parents. Cheatham testified he could see the

20 Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001).
21 Id. See also United States v. Slanina, 283 F.3d 670, 676 (5th Cir.), remanded on other grounds, 537 U.S. 802 (2002), on appeal after remand, 359 F.3d 356 (5th Cir. 2004) (use of passwords and locking office doors to restrict employer’s access to computer files is evidence of employee’s subjective expectation of privacy in those files).
door to Ray Andrus’ bedroom was open and asked Dr. Andrus whether he had access to the bedroom. Dr. Andrus testified he answered “yes” and told the officers he felt free to enter the room when the door was open, but always knocked if the door was closed.

Cheatham asked Dr. Andrus for consent to search the house and any computers in it. Dr. Andrus signed a written consent form indicating his willingness to consent to a premises and computer search. He led Cheatham into Ray Andrus’ bedroom to show him where the computer was located. After Dr. Andrus signed the consent form, Cheatham went outside to summon Kanatzar into the residence. Kanatzar went straight into Andrus’ bedroom and began assembling his forensic equipment. Kanatzar removed the cover from Andrus’ computer and hooked his laptop and other equipment to it. Dr. Andrus testified he was present at the beginning of the search but left the bedroom shortly thereafter. Kanatzar testified it took about ten to fifteen minutes to connect his equipment before he started analyzing the computer. Kanatzar used EnCase forensic software to examine the contents of the computer’s hard drive. The software allowed him direct access to the hard drive without first determining whether a user name or password were needed. He, therefore, did not determine whether the computer was protected by a user name or password prior to previewing the computer’s contents. Only later, when he took the computer back to his office for further analysis, did he see Ray Andrus’ user profile.[n.1]

Kanatzar testified he used EnCase to search for.jpg picture files. He explained that clicking on the images he retrieved allowed him to see the pathname for the image, tracing it to particular folders on the computer’s hard drive. This process revealed folder and file names suggestive of child pornography. Kanatzar estimated it took five minutes to see depictions of child pornography. At that point, however, Cheatham came back into the room, told Kanatzar that Ray Andrus was on his way home, and asked Kanatzar to stop the search. Kanatzar testified he shut down his laptop computer.

The district court determined Dr. Andrus’ consent was voluntary, but concluded Dr. Andrus lacked actual authority to consent to a computer search. The court based its actual authority ruling on its findings that Dr. Andrus did not know how to use the computer, had never used the computer, and did not know the user name that would have allowed him to access the computer.

The district court then proceeded to consider apparent authority. It indicated the resolution of the apparent authority claim in favor of the government was a “close call.” The court concluded the agents’ belief that Dr. Andrus had authority to consent to a search of the computer was reasonable up until the time they learned there was only one computer in the house. Because Cheatham instructed Kanatzar to suspend the search at that point, there was no Fourth Amendment violation.

Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority

[n.1] Kanatzar testified that someone without forensic equipment would need Ray Andrus’ user name and password to access files stored within Andrus’ user profile.
to consent to the search. When the property to be searched is an object or container, the relevant inquiry must address the third party's relationship to the object. The Supreme Court's most recent pronouncement on third party consent searches underscores that reasonableness calculations must be made in the context of social expectations about the particular item to be searched. The Court explained, "The constant element in assessing Fourth Amendment reasonableness in consent cases . . . is the great significance given to widely shared social expectations." For example, the Court said, "[W]hen it comes to searching through bureau drawers, there will be instances in which even a person clearly belonging on the premises as an occupant may lack any perceived authority to consent."

Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals' expectations of privacy in computers have been likened to their expectations of privacy in "a suitcase or briefcase." Password-protected files have been compared to a "locked footlocker inside the bedroom."

Because intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that "command[] a high degree of privacy."

The inquiry into whether the owner of a highly personal object has indicated a subjective expectation of privacy traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked. Determining whether a computer is "locked," or whether a reasonable officer should know a computer may be locked, presents a challenge distinct from that associated with other types of closed containers. Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the "off" position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected "user profile." See Oxford English Dictionary Online, http://dictionary.oed.com (last visited Dec. 22, 2006) (entry for "Password," definition 1.b.: defining "password" in the computing context as "[a] sequence of characters, known only to authorized persons, which must be keyed in to gain access to a particular computer, network, file, function, etc."). The presence of a password that limits access to the computer's contents may only be discovered by starting up the machine or attempting to access particular files on the computer as a normal user would.\(^\text{n.5}\)\(^24\)

Courts addressing the issue of third party consent in the context of computers, therefore, have examined officers' knowledge about password protection as an indication of whether a computer is "locked" in the way a footlocker would be. For example, in *Trulock* [v. Freeh, 275 F.3d 391 (4th Cir. 2001)], the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend's

\(^{24}\)\(^{n.5}\) The difficulty with seeing a "lock" on computer data is exacerbated by the forensic software sometimes used by law enforcement to conduct computer searches. The software, like the EnCase software used by Agent Kanatzar, allows user profiles and password protection to be bypassed.
computer files where the girlfriend told police she and her boyfriend shared the household computer but had separate password-protected files that were inaccessible to the other. The court in that case explained, “Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock’s password-protected files.” In *United States v. Morgan*, the Sixth Circuit viewed a wife’s statement to police that she and her husband did not have individual usernames or passwords as a factor weighing in favor of the wife’s apparent authority to consent to a search of the husband’s computer. 435 F.3d 660, 663 (6th Cir. 2006). A critical issue in assessing a third party’s apparent authority to consent to the search of a home computer, therefore, is whether law enforcement knows or should reasonably suspect because of surrounding circumstances that the computer is password protected.

In addition to password protection, courts also consider the location of the computer within the house and other indicia of household members’ access to the computer in assessing third party authority. Third party apparent authority to consent to a search has generally been upheld when the computer is located in a common area of the home that is accessible to other family members under circumstances indicating the other family members were not excluded from using the computer. In contrast, where the third party has affirmatively disclaimed access to or control over the computer or a portion of the computer’s files, even when the computer is located in a common area of the house, courts have been unwilling to find third party authority.

First, the officers knew Dr. Andrus owned the house and lived there with family members. Second, the officers knew Dr. Andrus’ house had internet access and that Dr. Andrus paid the Time Warner internet and cable bill. Third, the officers knew the email address bandrus@kc.rr.com had been activated and used to register on a website that provided access to child pornography. Fourth, although the officers knew Ray Andrus lived in the center bedroom, they also knew that Dr. Andrus had access to the room at will. Fifth, the officers saw the computer in plain view on the desk in Andrus’ room and it appeared available for use by other household members. Furthermore, the record indicates Dr. Andrus did not say or do anything to indicate his lack of ownership or control over the computer when Cheatham asked for his consent to conduct a computer search. It is uncontested that Dr. Andrus led the officers to the bedroom in which the computer was located, and, even after he saw Kanatzar begin to work on the computer, Dr. Andrus remained silent about any lack of authority he had over the computer. Even if Ray Andrus’ computer was protected with a user name and password, there is no indication in the record that the officers knew or had reason to believe such protections were in place.

Andrus argues his computer’s password protection indicated his computer was “locked” to third parties, a fact the officers would have known had they asked questions of Dr. Andrus prior to searching the computer. Under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous. In essence, by suggesting the onus was on the officers to ask about password protection prior to searching the computer, Andrus necessarily submits there is inherent ambiguity whenever police want to search a household computer and a third party has not affirmatively provided information about his own use of
the computer or about password protection. Andrus’ argument presupposes, however, that password protection of home computers is so common that a reasonable officer ought to know password protection is likely. Andrus has neither made this argument directly nor proffered any evidence to demonstrate a high incidence of password protection among home computer users. The dissent, however, is critical of this court because it neither makes the argument for Andrus nor supplies the evidence to support the argument. The key aspect of the dissent is its criticism of the majority for refusing to “take judicial notice that password protection is a standard feature of operating systems.” A judicially noticed fact is “one not subject to reasonable dispute in that it is either (1) generally known . . . or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Fed.R.Evid. 201(b). Although judicial notice may be taken *sua sponte*, it would be particularly inappropriate for the court to wander undirected in search of evidence irrefutably establishing the facts necessary to support the dissent’s conclusion regarding the absence of apparent authority: namely, that (a) password protection is a standard feature of most operating systems; (b) most users activate the standard password-protection feature; and (c) these are matters of such common knowledge that a reasonable officer would make further inquiry. Without a factual basis on which to proceed, we are unable to address the possibility that passwords create inherent ambiguities.[n.8]

Viewed under the requisite totality-of-the-circumstances analysis, the facts known to the officers at the time the computer search commenced created an objectively reasonable perception that Dr. Andrus was, at least, one user of the computer. That objectively reasonable belief would have been enough to give Dr. Andrus apparent authority to consent to a search. In this case, the district court found Agent Cheatham properly halted the search when further conversation with Dr. Andrus revealed he did not use the computer and that Andrus’ computer was the only computer in the house. These later revelations, however, have no bearing on the reasonableness of the officers’ belief in Dr. Andrus’ authority at the outset of the computer search.

McKay, Circuit Judge, dissenting.

I take issue with the majority’s implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party’s access to that password.

The development of computer password technology no doubt “presents a challenge distinct from that associated with other types of” locked containers. The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether

---

25 [n.8] If the factual basis were provided, law enforcement’s use of forensic software like EnCase, which overrides any password protection without ever indicating whether such protection exists, may well be subject to question. This, however, is not that case.
such passwords have been enabled does not “exacerbate[ ]” this difficulty; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were “shown to be commonplace, law enforcement’s use of forensic software like EnCase . . . may well be subject to question.” But the fact that a computer password “lock” may not be immediately visible does not render it unlocked. I appreciate that unlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers do exhibit outward signs of password protection: they display boot password screens, username/password log-in screens, and/or screen-saver reactivation passwords.[n.3]

The fact remains that EnCase’s ability to bypass security measures is well known to law enforcement. Here, ICE’s forensic computer specialist found Defendant’s computer turned off. Without turning it on, he hooked his laptop directly to the hard drive of Defendant’s computer and ran the EnCase program. The agents made no effort to ascertain whether such security was enabled prior to initiating the search. The testimony makes clear that such protection was discovered during additional computer analysis conducted at the forensic specialist’s office.

The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed. Prior to the computer search, the agents questioned Dr. Andrus about Ray Andrus’ status as a renter and Dr. Andrus’ ability to enter his 51-year-old son’s bedroom in order to determine Dr. Andrus’ ability to consent to a search of the room, but the agents did not inquire whether Dr. Andrus used the computer, and if so, whether he had access to his son’s password. At the suppression hearing, the agents testified that they were not immediately aware that Defendant’s computer was the only one in the house, and they began to doubt Dr. Andrus’ authority to consent when they learned this fact. The record reveals that, upon questioning, Dr. Andrus indicated that there was a computer in the house and led the agents to Defendant’s room. The forensic specialist was then summoned. It took him approximately fifteen to twenty minutes to set up his equipment, yet, bizarrely, at no point during this period did the agents inquire about the presence of any other computers. The consent form, which Dr. Andrus signed prior to even showing the agents Defendant’s computer, indicates that Dr. Andrus consented to the search of only a single “computer,” rather than computers. In addition, the local police officer accompanying the ICE agents heard Dr. Andrus tell his wife that the agents wanted to search Defendant’s computer, which would have caused a reasonable law enforcement official to question Dr. Andrus’ ownership and use of the computer.

The record reflects that, even prior to the agent’s arrival at the target home, the agents were cognizant of the ambiguity surrounding the search. The agents testified that they suspended their search due to doubts regarding Dr. Andrus’ ability to consent only after they learned that the internet service used by Defendant came bundled with the cable television service and was paid by Dr. Andrus. The district court noted, however, that the agents were aware of this fact

26 [n.3.] I recognize that the ability of users to program automatic log-ins and the capability of operating systems to “memorize” passwords poses potential problems, since these only create the appearance of a restriction without actually blocking access.
prior to the search, having subpoenaed the internet/cable records from the service provider prior to their “knock-and-talk.” Given the inexcusable confusion in this case, the circumstantial evidence is simply not enough to justify the agents’ use of EnCase software without making further inquiry.

Accordingly, in my view, given the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule, mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter’s knowledge of that password and joint access to the computer.

UNITED STATES v. FRANK GARY BUCKNER
473 F.3d 551 (4th Cir. 2007)

DIANA GRIBBON MOTZ, CIRCUIT JUDGE.

This criminal investigation began when the Grottoes, Virginia police department received a series of complaints regarding online fraud committed by someone using AOL and eBay accounts opened in the name Michelle Buckner. On July 28, 2003, police officers went to the Buckner residence to speak with Michelle, but only Frank Buckner was at home. The officers then left, asking Frank to have Michelle contact them. A short while later, Frank Buckner himself called the police, seeking more information about why they wanted to speak with Michelle. The police responded that they wanted to talk with her about some computer transactions. That evening, Michelle Buckner went to the police station and told officers that she knew nothing about any illegal eBay transactions, but that she did have a home computer leased in her name. She further stated that she only used the home computer occasionally to play solitaire.

The next day, July 29, police returned to the Buckner residence to speak further with Michelle about the online fraud. Frank Buckner was not present. Michelle again cooperated fully, telling the officers “to take whatever [they] needed” and that she “want[ed] to be as cooperative as she could be.” The computer Michelle had indicated was leased in her name was located on a table in the living room, just inside the front door of the residence. Pursuant to Michelle’s oral consent, the officers seized the leased home computer.

At the time the officers seized the computer, it was turned on and running, with the screen visibly lit. The officers did not, at this time, open any files or look at any information on the computer. Instead, with Michelle’s blessing, they shut down the computer and took its data — storage components for later forensic analysis. This analysis consisted of “mirroring” — that is, creating a copy of — the hard drive and looking at the computer’s files on the mirrored copy.

At a suppression hearing, Frank Buckner offered the only affirmative evidence on
the password issue, testifying that a password was required to use the computer. Buckner stated that he was the only person who could sign on to the computer and the only person who knew the password necessary to view files that he had created. Nothing in the record contradicts this testimony. Nor, however, is there any record evidence that the officers knew this information at the time they seized or searched the computer. Indeed, the evidence indicates that no officer, including the officer who conducted the search of the mirrored hard drive, ever found any indication of password protection. The Government’s evidence was that its forensic analysis software would not necessarily detect user passwords.\[n.1\]

In *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001), we held that a co-resident of a home and co-user of a computer, who did not know the necessary password for her co-user’s password-protected files, lacked the authority to consent to a warrantless search of those files. We likened these private files to a “locked box” within an area of common authority. Although common authority over a general area confers actual authority to consent to a search of that general area, it does not “automatically . . . extend to the interiors of every discrete enclosed space capable of search within the area.”

The logic of *Trulock* applies equally here. “By using a password,” Frank Buckner, like Trulock, “affirmatively intended to exclude . . . others from his personal files.” For this reason, “it cannot be said that” Buckner “assumed the risk” that a joint user of the computer, not privy to password-protected files, “would permit others to search his files.” Thus, Michelle Buckner did not have actual authority to consent to a search of her husband’s password-protected files because she did not share “mutual use, general access or common authority” over those files.

Michelle’s lack of actual authority, however, does not end our inquiry. Rather, it would be sufficient that Michelle had apparent authority to consent to the search at issue.

Frank Buckner contends that Michelle did not have common authority over his computer files — a fact that the officers must have known, according to Buckner, because Michelle had told them that she was not computer-savvy and that she only used the computer to play games.

Whether the officers reasonably believed that Michelle had authority to consent to a search of all the contents of the computer’s hard drive, however, depends on viewing these facts in light of the *totality* of the circumstances known to the officers at the time of the search. At that time, the officers knew that the computer was located in a common living area of the Buckners’ marital home, they observed that the computer was on and the screen lit despite the fact that Frank Buckner was not present, and they had been told that fraudulent activity had been conducted from that computer using accounts opened in Michelle’s name. The officers also knew that the machine was leased solely in Michelle’s name and that she had the ability to return the computer to the rental agency at any time, without Frank Buckner’s knowledge or consent.

\[n.1\] The parties agree that none of Frank Buckner’s files were encrypted. Nor is there any contention that the police officers *deliberately* used software that would avoid discovery of any existing passwords.
Furthermore, the officers did not have any indication from Michelle, or any of the attendant circumstances, that any files were password-protected. Even during the mirroring and forensic analysis processes, nothing the officers saw indicated that any computer files were encrypted or password-protected.[n.3]\(^{28}\) Despite Michelle’s suggestion that she lacked deep familiarity with the computer, the totality of the circumstances provided the officers with the basis for an objectively reasonable belief that Michelle had authority to consent to a search of the computer’s hard drive. Therefore, the police were justified in relying on Michelle’s consent to search the computer and all of its files, such that no search warrant was required.

\[\text{NOTE}\]

EnCase is a software tool made by Guidance Software that is used by many computer forensic examiners. See www.guidancesoftware.com. It is very configurable. Should courts construe the Fourth Amendment to require investigators to determine the existence of password protection prior to examining a digital device? In all situations or only when there is reason to suspect that the device is used by more than one person? If password protection is discovered, what may an investigator then be permitted to do?

\textbf{§ 7.4 FIFTH AMENDMENT PRIVILEGE: REQUIRING THE DISCLOSURE OF PASSWORDS, DECRYPTED FILES}

“Encryption involves the encoding of information, called ‘plaintext,’ into unreadable form, termed ‘ciphertext.’ The reverse process of transforming the ciphertext back into readable plaintext is called decryption. The purpose, of course, is to prevent anyone other than the user or intended recipient from reading private information.”\(^{29}\)

Encryption has become pervasive in our modern, technologically oriented society. In the home, encryption technology can be found in a multitude of devices. DVD and Blu-ray players perform decryption of encrypted, copyrighted movies. Wireless routers utilize encryption for security over the air. Every time someone uses the Internet to pay bills or to make purchases online, that person uses encryption technology. Commercially, companies use encryption to protect their data and to allow employees to securely access company networks from home through a Virtual Private Network.

\(^{28}\) [n.3] We do not hold that the officers could rely upon apparent authority to search while simultaneously using mirroring or other technology to intentionally avoid discovery of password or encryption protection put in place by the user.

\(^{29}\) John Duong, Note, The Intersection of the Fourth and Fifth Amendments in the Context of Encrypted Personal Data at the Border, 2 DREXEL L. REV. 313, 324 (2009). Copyright © 2009, Drexel Law Review. All rights reserved. Reprinted by permission.
Devices, both hardware and software, that utilize various encryption schemes are commonplace. Popular operating systems for computers, such as Microsoft Windows and Mac OS X, have some form of built-in encryption function that makes it easier for the public to use encryption technology. Commercial software is readily available to perform encryption of data and email. In addition to software-only solutions, hardware manufacturers have even launched products that have built-in, automatic encryption, making it virtually transparent to the end user who need not understand the underlying encryption technology in order to use it. One thing is certain: encryption exists to protect information, whether commercial or private.

Today’s encryption algorithms utilize complex mathematical routines to make it virtually impossible, given the computing power available today and in the foreseeable future, to “brute force” a passphrase. Even assuming that the government has the necessary computer processing power, there is still the question of whether it is even feasible given the resources necessary to perform the process of decryption. Without even knowing what the encrypted contents hold, it may be prohibitively expensive in time and cost to attempt decryption.30

---

IN RE GRAND JURY SUBPOENA TO SEBASTIEN BOUCHER
2009 US. Dist. Lexis 13006 (D. Vt. 2009)

WILLIAM K. SESSIONS, III, CHIEF JUDGE.

The Government appeals the United States Magistrate Judge’s Opinion and Order granting defendant Sebastien Boucher’s motion to quash a grand jury subpoena on the grounds that it violates his Fifth Amendment right against self-incrimination. The grand jury subpoena directs Boucher to provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006.

In its submission on appeal, the Government stated that it does not in fact seek the password for the encrypted hard drive, but requires Boucher to produce the contents of his encrypted hard drive in an unencrypted format by opening the drive before the grand jury. The Government stated that it intends only to require Boucher to provide an unencrypted version of the drive to the grand jury.

On December 17, 2006, Boucher and his father crossed the Canadian border into the United States at Derby Line, Vermont. A Custom and Border Protection inspector directed Boucher’s car into secondary inspection. The inspector conducting the secondary inspection observed a laptop computer in the back seat of Boucher’s car,

---

30 Id. at 324-28.
which Boucher acknowledged as his. The inspector searched the computer files and found approximately 40,000 images.

Based upon the file names, some of the files appeared to contain pornographic images, including child pornography. The inspector called in a Special Agent for Immigration and Customs Enforcement with experience and training in recognizing child pornography. The agent examined the computer and file names and observed several images of adult pornography and animated child pornography. He clicked on a file labeled “2yo getting raped during diaper change,” but was unable to open it. The “Properties” feature indicated that the file had last been opened on December 11, 2006.

After giving Boucher Miranda warnings, and obtaining a waiver from him, the agent asked Boucher about the inaccessible file. Boucher replied that he downloads many pornographic files from online newsgroups onto a desktop computer and transfers them to his laptop. He stated that he sometimes unknowingly downloads images that contain child pornography, but deletes them when he realizes their contents.

The agent asked Boucher to show him the files he downloads. Boucher navigated to drive “Z” of the laptop, and the agent began searching the Z drive. The agent located and examined several videos or images that appeared to meet the definition of child pornography.

The agent arrested Boucher, seized the laptop and shut it down. He applied for and obtained a search warrant for the laptop. In the course of creating a mirror image of the contents of the laptop, however, the government discovered that it could not find or open the Z drive because it is protected by encryption algorithms from the computer software “Pretty Good Protection,” which requires a password to obtain access. The government is not able to open the encrypted files without knowing the password. In order to gain access to the Z drive, the government is using an automated system which attempts to guess the password, a process that could take years.

The Fifth Amendment to the United States Constitution protects “a person . . . against being incriminated by his own compelled testimonial communications.” Fisher v. United States, 425 U.S. 391, 409 (1976). There is no question that the contents of the laptop were voluntarily prepared or compiled and are not testimonial, and therefore do not enjoy Fifth Amendment protection.

“Although the contents of a document may not be privileged, the act of producing the document may be.” “The act of production’ itself may implicitly communicate ‘statements of fact.’ By ‘producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.” United States v. Hubbell, 530 U.S. 27, 36 (2000). Thus, “the Fifth Amendment applies to acts that imply assertions of fact.” It is “the attempt to force [an accused] to ‘disclose the contents of his own mind’ that implicates the Self-Incrimination Clause.” Moreover, “[c]ompelled testimony that communicates information that may ‘lead to incriminating evidence’ is privileged even if the information itself is not inculpatory.”

At issue is whether requiring Boucher to produce an unencrypted version of his
laptop’s Z drive would constitute compelled testimonial communication. See In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992 (In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir.1993) (“Self-incrimination analysis now focuses on whether the creation of the thing demanded was compelled and, if not, whether the act of producing it would constitute compelled testimonial communication . . . regardless of ‘the contents or nature of the thing demanded.’”).

The act of producing documents in response to a subpoena may communicate incriminating facts “in two situations: (1) ‘if the existence and location of the subpoenaed papers are unknown to the government’; or (2) where production would ‘implicitly authenticate’ the documents.”

Where the existence and location of the documents are known to the government, “no constitutional rights are touched,” because these matters are a “foregone conclusion.” The Magistrate Judge determined that the foregone conclusion rationale did not apply, because the government has not viewed most of the files on the Z drive, and therefore does not know whether most of the files on the Z drive contain incriminating material. Second Circuit precedent, however, does not require that the government be aware of the incriminatory contents of the files; it requires the government to demonstrate “with reasonable particularity that it knows of the existence and location of subpoenaed documents.”

Thus, where the government, in possession of a photocopy of a grand jury target’s daily calendar, moved to compel compliance with a subpoena for the original, the Second Circuit ruled that no act of production privilege applied. The existence and location of the calendar were foregone conclusions, because the target had produced a copy of the calendar and testified about his possession and use of it.

The target’s production of the original calendar was also not necessary to authenticate it; the government could authenticate the calendar by establishing the target’s prior production of the copy and allowing the trier of fact to compare the two.

Boucher accessed the Z drive of his laptop at the ICE agent’s request. The ICE agent viewed the contents of some of the Z drive’s files, and ascertained that they may consist of images or videos of child pornography. The Government thus knows of the existence and location of the Z drive and its files. Again providing access to the unencrypted Z drive “adds little or nothing to the sum total of the Government’s information” about the existence and location of files that may contain incriminating information.

Boucher’s act of producing an unencrypted version of the Z drive likewise is not necessary to authenticate it. He has already admitted to possession of the computer, and provided the Government with access to the Z drive. The Government has submitted that it can link Boucher with the files on his computer without making use of his production of an unencrypted version of the Z drive, and that it will not use his act of production as evidence of authentication.

Because Boucher has no act of production privilege to refuse to provide the grand jury with an unencrypted version of the Z drive of his computer, his motion to quash the subpoena (as modified by the Government) is denied. Boucher is directed to
provide an unencrypted version of the Z drive viewed by the ICE agent. The Government may not make use of Boucher’s act of production to authenticate the unencrypted Z drive or its contents either before the grand jury or a petit jury.

NOTES


Unlike physical evidence, which exists independently from the person, there is no such separation between a person and his or her passphrase. The passphrase is inherently intertwined within the chasms of the mind of the individual. In other words, being compelled to produce a passphrase involves mining and extracting the contents of one’s mind and that act itself inherently involves revealing the contents of that mind, which makes it a testimonial communication. This link simply cannot be conceptually severed.

2. Duong, in his Note, also argues:

[T]he District Court [in Boucher] erred . . . by claiming that the government already knew “of the existence and location of the Z drive and its files.” This is precisely the kind of fishing expedition that the Hubbell Court rejected. In Hubbell, the Supreme Court stated that a broad-based belief of certain materials is not enough for application of the forgone conclusion doctrine. The government must be able to specify that it knew such materials existed and where they were located. In this case, the government only knew the existence and location of some of the child pornography files. Contrary to the District Court’s assertion that the contents of the entire decrypted Z drive would not add much to the sum total of the government’s knowledge, it could in fact add considerably if Boucher had many more incriminating files than were previously viewed by the Customs agents. The District Court should have performed the same analysis and held that Boucher must only produce the files of which the government already had prior knowledge.

Id. at 355 n.210.

3. An Ethical quandary? When faced with the order by the court in Boucher, as his attorney, what advice could you ethically provide? What are the consequences of refusing to comply with the court order vs. a possible conviction for child pornography charges?

4. The reasonableness of the search and seizure of computers at the International border is considered in Chapter 10.
Chapter 8

CELL PHONES, OTHER MOBILE DIGITAL DEVICES, AND TRADITIONAL FOURTH AMENDMENT DOCTRINE PERMITTING WARRANTLESS SEARCHES

Mobile digital devices are everywhere and have wide ranging capabilities. This chapter pays particular attention to one such device — the cell phone — and some of the circumstances where the police have searched the contents of those devices. The legal analysis is as complex as the modern technology that goes into a cell phone.

§ 8.1 SEARCH INCIDENT TO ARREST

1. Basic Principles

The application of the search incident to arrest principle is one of the main consequences of an arrest. It involves a significant intrusion upon the person of the suspect, as well as the suspect’s belongings within the area under the suspect’s control. The evidentiary results of such searches often have a significant influence on the course of any subsequent criminal proceedings. Searches incident to arrest are a common form of search and, given the development of modern police forces and the statutory expansion of the number of crimes, such searches now apply to large numbers of criminal suspects. Given the ubiquity of portable digital devices carried on or about one’s person in today’s world, the search incident to arrest doctrine has potentially vast application.

Search incident to arrest principles have undergone significant evolution since the imposition of the exclusionary rule on federal authorities in Weeks v. United States, 232 U.S. 383 (1914), which itself recognized the propriety of a search incident to arrest. First, the nature of the justification for such searches have had several iterations. Many cases prior to Robinson v. United States, 414 U.S. 218 (1973), viewed searches incident to arrest in terms of an exception to the warrant requirement, which intimated an exigent circumstances rationale and, perhaps, a need to justify the search in each case. While not all of the United States Supreme Court’s cases reflected that view, a dispositive doctrinal shift in the underlying justification for searches incident to arrest occurred in Robinson, where the Court stated:

A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. It is the
fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a “reasonable” search under that Amendment.

In *Robinson*, which involved the arrest of a person for driving after his license had been revoked, the Court adopted a “categorical” search incident to arrest rule: it applied to all arrests, regardless of the underlying factual circumstances. In so ruling, the Court rejected a case-by-case inquiry. *Robinson’s* view has prevailed in subsequent decades, although language in *Arizona v. Gant* (reproduced *infra*) recently cast new doubt on that view.

A second consideration concerns the purpose of the search that is being authorized by the fact of the arrest. One aspect, always accepted, is that such searches serve to protect the safety of the officer by allowing the police to search for weapons and other objects that may be used to attack the officer. Thus, for example, in *Chimel v. California*, 395 U.S. 752 (1969), the Court observed: “When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer’s safety might well be endangered, and the arrest itself frustrated.” The cases have also recognized a second purpose for a search incident to arrest: to recover evidence. It is here that much conflict, ambiguity, and changes of course permeate the case law. One view is that the permissible search is for evidence of the crime committed. The broader and current view (outside of the vehicle context) is that the search may be for any evidence of any crime. Depending on which view is adopted, the permitted scope of a search incident to arrest will vary.

### 2. Permissible Objects Sought

While older case law was somewhat unclear whether, other than weapons, the objects permissibly seized pursuant to the arrest had to relate to the offense for which the arrest was made, modern Supreme Court jurisprudence, with few exceptions, does not impose any limits on the search based on the types of objects sought. *United States v. Robinson*, 414 U.S. 218 (1973), is the leading case. Robinson was arrested for operating a motor vehicle after his operator’s permit had been revoked. The arresting officer subjected him to a full search. Upon feeling an object in one of Robinson’s coat pockets, the officer removed it. The object was a “crumpled up cigarette package,” which the officer opened, revealing gelatin capsules of white powder that, upon later analysis, proved to be heroin. The *Robinson* Court established bright-line authority to search, with no limitations based on the type of crime or the likelihood of finding additional evidence of that
crime during the search. Subject to few exceptions, the effect of the Court’s view is to afford complete discretion to the police as to the objects sought during the search. The ramifications are dramatic: all objects — from the clothing worn by the suspect\(^4\) to the contents of wallets\(^5\) — are subject to search.

### 3. Cell Phone Searches Incident to Arrest

May the digital contents of cell phones and similar devices be searched incident to arrest? The next case in the reading, *State v. Smith*, examines that question. To date, *Smith* is the minority view.

#### STATE v. ANTWAUN SMITH

920 N.E.2d 949 (Ohio 2009)

**LANZINGER, J.**

On January 21, 2007, Wendy Thomas Northern was transported to Miami Valley Hospital after a reported drug overdose. While at the hospital, she was questioned by Beavercreek police. Northern agreed to call her drug dealer, whom she identified as appellant, Antwaun Smith, to arrange for the purchase of crack cocaine at her residence.

That evening, the Beavercreek police arrested Smith at Northern’s residence. During the arrest, police searched Smith and found a cell phone on his person. The arresting officer put the cell phone in his pocket and placed Smith in a cruiser, then searched the scene for evidence.

While the record does not show exactly when they first searched Smith’s cell phone, at some point police discovered that the call records and phone numbers confirmed that Smith’s cell phone had been used to speak with Northern. There was testimony that at least a portion of the search took place when officers returned to the police station and were booking into evidence the items seized from the crime scene.

In part, whether the warrantless search of a cell phone passes constitutional muster depends upon how a cell phone is characterized, because whether a search is determined to be reasonable is always fact-driven.

#### 1. The Approach of *United States v. Finley*

In *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007), the Fifth Circuit upheld the district court’s denial of defendant’s motion to suppress call records and text messages retrieved from his cell phone. Finley was arrested during a traffic stop after a passenger in his van sold methamphetamine to an informant. During the search incident to the arrest, police found a cell phone in Finley’s pocket. He was


\(^5\) E.g., *United States v. Watson*, 669 F.2d 1374 (11th Cir. 1982).
taken along with his passenger to the passenger’s house, where other officers were
conducting a search. While Finley was being questioned there, officers examined
the cell phone’s call records and text messages, finding evidence that appeared to
be related to narcotics use and drug trafficking.

In upholding the search, the Fifth Circuit analogized Finley’s cell phone to a closed
container found on an arrestee’s person, which may be searched.

2. The Approach of United States v. Park

The United States District Court for the Northern District of California granted a
defendant’s motion to suppress the warrantless search of his cell phone. United
officers observed Park entering and leaving a building that they had under
surveillance and for which they had obtained a search warrant. When they
executed the warrant and searched the building, they found evidence of an indoor
marijuana-cultivation operation. They arrested Park and took him to booking,
where they searched him and found a cell phone. Before turning over the cell
phone to the booking officer, the arresting officer recorded names and phone
numbers found in Park’s cell phone.

This district court reasoned that modern cell phones “have the capacity for storing
immense amounts of private information” and thus likened the devices to laptop
computers, in which arrestees have significant privacy interests, rather than to
address books or pagers found on their persons, in which they have lesser privacy
interests. Because the search of the cell phone’s contents was not conducted out of
concern for the officer’s safety or to preserve evidence, the court found that it did
not fall under the search-incident-to-arrest exception and that the officers should
have obtained a warrant to conduct the search.

3. Closed Containers

Objects falling under the banner of “closed container” have traditionally been
physical objects capable of holding other physical objects. Indeed, the United
States Supreme Court has stated that in this situation, “container” means “any
object capable of holding another object.” New York v. Belton (1981), 453 U.S. 454,
460. One such example is a cigarette package containing drugs found in a person’s
pocket, as in United States v. Robinson (1973), 414 U.S. 218.

We acknowledge that some federal courts have likened electronic devices to closed
containers. Each of these cases, however, fails to consider the Supreme Court’s
definition of “container” in Belton, which implies that the container must actually
have a physical object within it. Additionally, the pagers and computer memo books
of the early and mid 1990s bear little resemblance to the cell phones of today. Even
the more basic models of modern cell phones are capable of storing a wealth of
digitized information wholly unlike any physical object found within a closed
container. We thus hold that a cell phone is not a closed container for purposes of
a Fourth Amendment analysis.
4. Legitimate Expectation of Privacy

Since cell phones are not closed containers, the question becomes how they should be classified. Given the continuing rapid advancements in cell phone technology, we acknowledge that there are legitimate concerns regarding the effect of allowing warrantless searches of cell phones, especially so-called smart phones, which allow for high-speed Internet access and are capable of storing tremendous amounts of private data. While it is apparent from the record that Smith's cell phone could not be called a smart phone with advanced technological capability, it is clear from the record that Smith's cell phone had phone, text messaging, and camera capabilities. While the dissent argues that Smith's phone is merely a “conventional one,” we note that in today's advanced technological age many “standard” cell phones include a variety of features above and beyond the ability to place phone calls. Indeed, like Smith’s phone, many cell phones give users the ability to send text messages and take pictures. Other modern “standard” cell phones can also store and transfer data and allow users to connect to the Internet. Because basic cell phones in today's world have a wide variety of possible functions, it would not be helpful to create a rule that requires officers to discern the capabilities of a cell phone before acting accordingly.

Given their unique nature as multifunctional tools, cell phones defy easy categorization. On one hand, they contain digital address books very much akin to traditional address books carried on the person, which are entitled to a lower expectation of privacy in a search incident to an arrest. On the other hand, they have the ability to transmit large amounts of data in various forms, likening them to laptop computers, which are entitled to a higher expectation of privacy.

But cell phones are neither address books nor laptop computers. They are more intricate and multifunctional than traditional address books, yet they are still, in essence, phones, and thus they are distinguishable from laptop computers. Although cell phones cannot be equated with laptop computers, their ability to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain. Once the cell phone is in police custody, the state has satisfied its immediate interest in collecting and preserving evidence and can take preventive steps to ensure that the data found on the phone are neither lost nor erased. But because a person has a high expectation of privacy in a cell phone’s contents, police must then obtain a warrant before intruding into the phone's contents.

Although the dissent maintains that this case can be decided on the basis of traditional Fourth Amendment principles governing searches incident to arrest, the dissent fails to recognize that the justifications behind allowing a search incident to arrest are officer safety and the preservation of evidence. There is no evidence that either justification was present in this case. A search of the cell phone’s contents was not necessary to ensure officer safety, and the state failed to present any evidence that the call records and phone numbers were subject to imminent destruction. We therefore hold that because a cell phone is not a closed container, and because an individual has a privacy interest in the contents of a cell phone that goes beyond the privacy interest in an address book or pager, an officer
may not conduct a search of a cell phone's contents incident to a lawful arrest without first obtaining a warrant.

CUPP, J., dissenting.

The majority needlessly embarks upon a review of cell phone capabilities in the abstract in order to announce a sweeping new Fourth Amendment rule that is at odds with decisions of other courts that have addressed similar questions.

In my view, this case deals with a straightforward, well-established principle: “[I]n the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a ‘reasonable’ search under that Amendment.” In Robinson, the United States Supreme Court upheld admission into evidence of a cigarette package containing drugs, which was found as part of a search incident to Robinson’s arrest. And as in United States v. Edwards (1974), 415 U.S. 800, 803, “searches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention.”

In this case, there is no dispute that the arrest of Smith was lawful. During the search of Smith incident to his arrest for drug trafficking and other offenses, the officers located his cell phone on his person. There is no evidence that this phone was anything other than a conventional one, rather than a “smart phone” with advanced technological capability.

The police later (at the police station) searched Smith’s cell phone’s address book and call list. A cell phone’s digital address book is akin to traditional address books carried on the person. Courts have upheld police officers’ search of an address book found on an arrestee’s person during a search incident to a lawful arrest. The phone’s call list is similar, showing a list of telephone numbers that called to or were called from the phone.

Thus, I would hold that the search here — which resembles police officers’ search of a traditional address book found on the person of an arrestee during a search incident to arrest — is permissible under the Fourth Amendment.

It would be unworkable to devise a rule that required police to determine the particular cell phone’s storage capacity, and the concomitant risk that telephone numbers stored on the phone could be lost over time, before searching the phone’s address book or call list. I would hold that a search of an arrestee’s cell phone’s address book and call list is permissible as part of a search incident to arrest without first requiring police to determine the cell phone’s storage capabilities.

I see no need here to delve into a wide-ranging examination of the capabilities of different types of cell phones and other electronic devices. The majority bases its broad holdings on its estimation of the possible capabilities of other cell phones and computers. But here, only the address book and call records were admitted into evidence. The issue of a more in-depth warrantless search of “data within a cell phone” is not before us.
4. Location of the Search

The scope of a search incident to arrest includes the location where the accused is arrested but the right to search does not extend to other places. There is considerable fiction involved in fixing the place of search. The permissible location for searches incident to arrest is generally the spot where the police first detained the person, even if he or she has been moved some distance thereafter or is sitting handcuffed in a vehicle. This result is widely criticized by commentators because, factually, there is usually no basis for believing that the suspect could obtain a weapon or destroy evidence in the area searched; yet, factual considerations are no longer the inquiry after Robinson, which substituted a categorical rule for any case-by-case analysis. The fictionalized area of control at least prevents the police from using the suspect as a “walking search warrant” by moving him into a house and from room to room to conduct a warrantless search of the house.

The Court has often remarked that the search must be contemporaneous or “substantially contemporaneous with the arrest” both as to time and place. As with other features of the search incident to arrest rule, there is considerable debate as to the meanings of those requirements. The Supreme Court seemed to abandon the contemporaneous limitation for searches of the person incident to a lawful arrest in United States v. Edwards, 415 U.S. 800 (1974), which involved the search of the defendant’s clothing at the jail where he was incarcerated ten hours after he was arrested. The Edwards Court stated: “It is . . . plain that searches and seizures that could be made on the spot at the time of the arrest may legally be conducted later when the accused arrives at the place of detention.” The Court broadly opined:

[O]nce the accused is lawfully arrested and is in custody, the effects in his possession at the place of detention that were subject to search at the time and place of his arrest may lawfully be searched and seized without a warrant even though a substantial period of time has elapsed between the arrest and subsequent administrative processing, on the one hand, and the taking of the property for use as evidence, on the other. This is true where the clothing or effects are immediately seized upon arrival at the jail, held

---

10 E.g., Stoner v. California, 376 U.S. 483, 486 (1964) (invalidating warrantless search conducted two days before arrest). Cf. Preston v. State, 784 A.2d 601 (Md. Ct. Spec. App. 2001) (Collecting cases and observing: “Searches have been deemed to be ‘essentially contemporaneous’ with an arrest when made within a few minutes after the arrest even if the suspect, at the time of a search, has been placed in a police cruiser and handcuffed.” Rejecting a delay of “at least two or three hours,” the court added that “we have found none, where any court has held that a search that takes place two or more hours after an arrest is nevertheless ‘essentially contemporaneous’ with that arrest.”).
11 United States v. Hrasky, 453 F.3d 1099 (8th Cir. 2006).
under the defendant’s name in the “property room” of the jail, and at a later
time searched and taken for use at the subsequent criminal trial. The result
is the same where the property is not physically taken from the defendant
until sometime after his incarceration.

Edwards' reasoning was a blend of various justifications for the permissibility of the
search, including search incident to arrest, search incident to incarceration,
inventory, and a probable cause-based analysis combined with the fact that
Edwards and his property were rightfully in police custody. The Edwards Court
“perceived little difference” in a search at the scene of the arrest and at the police
station, with “similar” justifications supporting a search at either place. The Court
also justified the delayed search based on a factual analysis of the case:

[T]he police had probable cause to believe that the articles of clothing
[Edwards] wore were themselves material evidence of the crime for which
he had been arrested. But it was late at night; no substitute clothing was
then available for Edwards to wear, and it would certainly have been
unreasonable for the police to have stripped respondent of his clothing and
left him exposed in his cell throughout the night. When the substitutes were
purchased the next morning, the clothing he had been wearing at the time
of arrest was taken from him and subjected to laboratory analysis. This was
no more than taking from respondent the effects in his immediate
possession that constituted evidence of crime. This was and is a normal
incident of a custodial arrest, and reasonable delay in effectuating it does
not change the fact that Edwards was no more imposed upon than he could
have been at the time and place of the arrest or immediately upon arrival
at the place of detention. The police did no more . . . than they were
entitled to do incident to the usual custodial arrest and incarceration.

In United States v. Chadwick, 433 U.S. 1 (1977), which did not involve the search
incident to arrest doctrine because the object searched — a footlocker located in the
trunk of a vehicle — was outside the defined area of an arrestee's control, the Court
nonetheless observed:

[W]arrantless searches of luggage or other property seized at the time of
an arrest cannot be justified as incident to that arrest either if the “search
is remote in time or place from the arrest,” or no exigency exists. Once law
enforcement officers have reduced luggage or other personal property not
immediately associated with the person of the arrestee to their exclusive
control, and there is no longer any danger that the arrestee might gain
access to the property to seize a weapon or destroy evidence, a search of
that property is no longer an incident of the arrest.

Here the search was conducted more than an hour after federal agents had
gained exclusive control of the footlocker and long after respondents were
securely in custody; the search therefore cannot be viewed as incidental to
the arrest or as justified by any other exigency.

In a footnote, the Chadwick Court sought to distinguish Edwards: “Unlike searches
of the person, searches of possessions within an arrestee’s immediate control cannot
be justified by any reduced expectations of privacy caused by the arrest.”
Given the mixture of rationales supporting the Edwards decision, combined with Chadwick's interpretation of that case and the lack of any guidance in subsequent Supreme Court case law, it is not surprising that the lower court decisions are in conflict. What appears clear after Edwards is that, using any of its alternative rationales, a full search of an arrestee at the police station is permitted. But what about other objects seized at the time of the arrest and transported to the station? Under current Supreme Court doctrine, many objects may be searched under the inventory search doctrine. Some courts ask whether the administrative processes incident to arrest are still continuing at the time the search occurs. Putting those considerations aside, lower courts have grappled with the impact of the Edwards and Chadwick “contemporaneous” requirement for a search incident to arrest. “Cases decided subsequent to Chadwick have distinguished between searches of items ‘closely associated with the arrestee’ made at the police station and searches of luggage and other articles of personal property not immediately associated with the person of the arrestee. The former may be searched long after the arrest, while the latter may be searched only incident to the suspect’s arrest.” There has arisen a dubious jurisprudence of containers, with fine distinctions between types of containers and their closeness of association with the person. Thus, cases have determined whether searches of wallets, purses, luggage, and backpacks are permissible.

PEOPLE v. GREGORY DIAZ
81 Cal. Rptr. 3d 215 (Cal. Ct. App. 2008), aff’d, 244 P.3d 501 (Cal. 2011)

Perren, J.

Gregory Diaz appeals the judgment entered after he pled guilty to transportation of a controlled substance, Ecstasy. He contends that the delayed warrantless search of his cell phone violated the Fourth Amendment because the phone was a

13 E.g., United States v. Finley, 477 F.3d 250, 260 n.7 (5th Cir. 2007); United States v. Ruigomez, 702 F.2d 61, 66 (5th Cir. 1983).
14 Preston v. State, 784 A.2d 601 (Md. Ct. Spec. App. 2001) (collecting cases). See United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (“Finley’s cell phone does not fit into the category of ‘property not immediately associated with [his] person’ because it was on his person at the time of his arrest.”).
15 The Court, in other aspects of Fourth Amendment jurisprudence, had at one time attempted to create a distinction between containers but ultimately rejected that view as without logical support. See Thomas K. Clancy, The Fourth Amendment: Its History and Interpretation § 4.6.1. (2008).
16 United States v. Phillips, 607 F.2d 808, 809-10 (8th Cir. 1979) (search of defendant’s wallet at police station “substantial period of time” after arrest was valid search incident to arrest).
17 Curd v. City Court of Judsonia, 141 F.3d 839 (8th Cir. 1998) (plaintiff’s purse permissibly searched at police station fifteen minutes after arrest).
18 United States v. $639,558 in U.S. Currency, 955 F.2d 712, 715-16 (D.C. Cir. 1992) (luggage search half an hour after arrest not contemporaneous); State v. Calegar, 661 P.2d 311, 315-16 (Idaho 1983) (suitcase seized from automobile in which defendant was arrested permissibly searched at police station).
“possession[,] within an arrestee’s immediate control,” instead of an item “spacially limited to the person of the arrestee,” as those terms are defined by United States v. Chadwick (1977) 433 U.S. 1, 16, footnote 10, and United States v. Edwards (1974) 415 U.S. 800, 810. We conclude that the cell phone was immediately associated with Diaz’s person at the time of his arrest, and was therefore properly subjected to a delayed warrantless search.

At 2:50 p.m. on April 25, 2007, Diaz participated in a controlled buy of six Ecstasy pills. Diaz drove Lorenzo Hampton to the location in Thousand Oaks, and waited while Hampton and a confidential informant conducted the transaction in the back seat of his car. Diaz and Hampton were arrested shortly thereafter. When Diaz was searched at the scene, a small amount of marijuana was recovered from his back pocket. Diaz also had a cell phone in his possession, but it was not seized at that time.

Diaz was transported to the East County Sheriff’s Station. At approximately 4:00 p.m., Diaz’s cell phone was seized from his person and placed with the other evidence that had been collected. At 4:18 p.m., Diaz was interviewed by Detective Victor Fazio of the Ventura County Sheriff’s Department. Diaz waived his Miranda rights and denied any involvement in the incident. At about 4:23 p.m., and while Diaz was still being interrogated, Detective Fazio retrieved Diaz’s cell phone, searched the text message folder, and found a recent message addressed to Hampton stating “6 4 80.” Based on his training and experience, the detective believed that this message referred to 6 Ecstasy pills for the price of $80. Diaz admitted his participation in the crime when confronted with this information.

Diaz does not dispute that his cell phone was properly seized incident to his arrest and that the police could have searched it contemporaneous with the arrest. He contends, however, that the search of his cell phone approximately 90 minutes after his arrest violated the Fourth Amendment’s requirement that a warrant be obtained for delayed searches of “possessions within an arrestee’s immediate control.” While he acknowledges that items “immediately associated with the person of the arrestee” are properly subject to delayed warrantless searches, he argues that cell phones should be afforded greater constitutional protection than other items an arrestee might carry on his or her person, such as wallets, letters, or address books, because they “have the capacity to store tremendous quantities of personal information.” He also asserts that cell phones should be characterized differently from other items associated with the person of an arrestee because they are “no more likely to be inside a person’s pocket than inside a briefcase, backpack, or purse, or on a car seat or table, or plugged into a power source, or stashed inside any manner of separate bags or carrying containers.”

Cell phones may contain personal information, but so do wallets, purses and the like. The fact that electronic devices are capable of storing vast amounts of private information does not give rise to a legitimate heightened expectation of privacy where, as here, the defendant is subject to a lawful arrest while carrying the device on his person.[n.2] Whether Diaz could have kept his cell phone in a briefcase or backpack is of no moment. Because he had the phone on his person at the time of

---

[n.2] The record does not disclose whether Diaz’s phone was in his hand, a pocket of his clothing,
his arrest, it was taken “out of the realm of protection from police interest” for a reasonable amount of time following the arrest.

Diaz also contends that “a cell phone text message search exceeds the original rationale for searches incident to arrest: to ensure officer safety and to preserve evidence that could be concealed or destroyed.” The United States Supreme Court has recognized, however, that “[a] police officer’s determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search. The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect. A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a ‘reasonable’ search under that Amendment.” In any event, “[t]he need to preserve evidence is underscored where evidence may be lost due to the dynamic nature of the information stored on and deleted from cell phones or pagers.”

**QUESTION**

Assuming that the court is applying traditional Fourth Amendment doctrine and is not creating “special” rules for digital devices and also assuming that the cell phone was in the arrestee’s pocket and accessed at the scene of the arrest, are any or all of the following actions by the officer permissible:24

1. activates touch screen to view phone’s contents
2. clicks on internet browser icon
3. clicks on toolbar to find bookmarks link
4. finds suspicious-looking bookmark labeled “porn pictures”
5. clicks on bookmark to bring up webpage
6. webpage contains series of icons including “members” button; clicks image
7. brings up “members” page, which already has the account number / password entered

or elsewhere on his person at the time it was seized. It is undisputed, however, that the phone was “on his person.”

---

8. clicks “submit” button, which utilizes the saved account information / password to bring up the content of a website

9. sees pictures and message function; account owner has new messages

*Here’s a hint:* An iPhone is a smartphone sold by Apple. It integrates cell phone technology, iPod, camera, text messaging, email, and Web browsing. Data and applications can be sent to this device via a wireless signal or Apple’s iTunes software, which is used to organize music, videos, photos, and applications. Are all of those functions accessible under traditional search incident to arrest doctrine?

5. **Scope: Areas Within the Arrestee’s “Control”**

Throughout much of the twentieth century, the Court struggled to establish the proper scope of the area around the arrestee that may be searched. In the 1969 case of *Chimel v. California*, 395 U.S. 752 (1969), the Court created a rule that has since prevailed:

When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer’s safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee’s person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule. A gun on a table or in a drawer in front of one who is arrested can be as dangerous to the arresting officer as one concealed in the clothing of the person arrested. There is ample justification, therefore, for a search of the arrestee’s person and the area “within his immediate control” — construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.

There is no comparable justification, however, for routinely searching any room other than that in which an arrest occurs — or, for that matter, for searching through all the desk drawers or other closed or concealed areas in that room itself. Such searches, in the absence of well-recognized exceptions, may be made only under the authority of a search warrant. The “adherence to judicial processes” mandated by the Fourth Amendment requires no less.

Since *Chimel*, the scope of the search incident to arrest rule’s application to areas beyond the arrestee’s person has been settled — at least rhetorically. That scope is defined to include only those areas within the arrestee’s “immediate control,” which is in turn defined as those areas where he “might reach in order to grab a weapon or evidentiary item.” This grab area has often been referred to as the

---

25 *See* PC MAGAZINE, Encyclopedia, available at http://www.pcmag.com/encyclopedia term/0,2542,t=iPhone&i=45364,00.asp.

26 *See,* e.g., Thornton v. United States, 541 U.S. 615 (2004) (“Although easily stated, the *Chimel* principle had proved difficult to apply in specific cases.”).
“wingspan” or “lunge area.” Unlike many aspects of the modern search incident to arrest rule, the area to be searched (with the exception of vehicle searches), is a fact-based inquiry in each case. However, the area of immediate control is measured as of the moment of arrest and not at the moment of search. Hence, as with many of the principles regulating searches incident to arrest, there is a significant amount of fiction in deciding what the area of immediate control is: “Because police officers virtually always restrain the individual immediately after placing him under arrest, as they are trained to do, an arrestee generally will be handcuffed or locked in a squad car, or both, before any search . . . takes place.”

6. Scope: Vehicle Searches Incident to Arrest

When a person who has been in a vehicle is arrested, what is the proper area of “immediate control” to be searched incident to that arrest? To establish a workable rule, the Court in *New York v. Belton*, 453 U.S. 454 (1981), held that, as an incident to arrest of an automobile occupant, the police may search the entire passenger compartment of the car, including any open or closed containers, but not the trunk. The *Belton* Court believed that the entire passenger compartment of a vehicle was “in fact generally, even if not inevitably,” the area where a person could reach to grab a weapon or evidence. It therefore held: “when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile.” The next case in the reading, *Arizona v. Gant*, while claiming not to overrule *Belton*, has effectively done so. *Gant* is a major new Fourth Amendment case, decided by a 5-4 vote. Excerpted here are the two holdings of the majority opinion.

---

**ARIZONA v. RODNEY JOSEPH GANT**

**Justice Stevens** delivered the opinion of the Court.

Acting on an anonymous tip that the residence at 2524 North Walnut Avenue was being used to sell drugs, Tucson police officers Griffith and Reed knocked on the front door and asked to speak to the owner. Gant answered the door and, after identifying himself, stated that he expected the owner to return later. The officers left the residence and conducted a records check, which revealed that Gant's

---


28 The *Belton* Court stated:
“Container” here denotes any object capable of holding another object. It thus includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like. Our holding encompasses only the interior of the passenger compartment of an automobile and does not encompass the trunk.
driver’s license had been suspended and there was an outstanding warrant for his arrest for driving with a suspended license.

When the officers returned to the house that evening, they found a man near the back of the house and a woman in a car parked in front of it. After a third officer arrived, they arrested the man for providing a false name and the woman for possessing drug paraphernalia. Both arrestees were handcuffed and secured in separate patrol cars when Gant arrived. The officers recognized his car as it entered the driveway, and Officer Griffith confirmed that Gant was the driver by shining a flashlight into the car as it drove by him. Gant parked at the end of the driveway, got out of his car, and shut the door. Griffith, who was about 30 feet away, called to Gant, and they approached each other, meeting 10-to-12 feet from Gant’s car. Griffith immediately arrested Gant and handcuffed him.

Because the other arrestees were secured in the only patrol cars at the scene, Griffith called for backup. When two more officers arrived, they locked Gant in the backseat of their vehicle. After Gant had been handcuffed and placed in the back of a patrol car, two officers searched his car: One of them found a gun, and the other discovered a bag of cocaine in the pocket of a jacket on the backseat.

In *Chimel*, we held that a search incident to arrest may only include “the arrestee’s person and the area ‘within his immediate control’ — construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.” That limitation, which continues to define the boundaries of the exception, ensures that the scope of a search incident to arrest is commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy. If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply.

In *Belton*, we considered *Chimel’s* application to the automobile context.... [W]e held that when an officer lawfully arrests “the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of the automobile” and any containers therein. That holding was based in large part on our assumption “that articles inside the relatively narrow compass of the passenger compartment of an automobile are in fact generally, even if not inevitably, within ‘the area into which an arrestee might reach.’ ”

To read *Belton* as authorizing a vehicle search incident to every recent occupant’s arrest would untether the rule from the justifications underlying the *Chimel* exception. Accordingly, we reject this reading of *Belton* and hold that the *Chimel* rationale authorizes police to search a vehicle incident to a recent occupant’s arrest only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search.[n.4]29

We also conclude that circumstances unique to the vehicle context justify a search

---

29 [n.4] Because officers have many means of ensuring the safe arrest of vehicle occupants, it will be the rare case in which an officer is unable to fully effectuate an arrest so that a real possibility of access to the arrestee’s vehicle remains. But in such a case a search incident to arrest is reasonable under the Fourth Amendment.
incident to a lawful arrest when it is “reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.” In many cases, as when a recent occupant is arrested for a traffic violation, there will be no reasonable basis to believe the vehicle contains relevant evidence. But in others, including *Belton*, the offense of arrest will supply a basis for searching the passenger compartment of an arrestee’s vehicle and any containers therein.

Neither the possibility of access nor the likelihood of discovering offense-related evidence authorized the search in this case. Unlike in *Belton*, which involved a single officer confronted with four unsecured arrestees, the five officers in this case outnumbered the three arrestees, all of whom had been handcuffed and secured in separate patrol cars before the officers searched Gant’s car. Under those circumstances, Gant clearly was not within reaching distance of his car at the time of the search. An evidentiary basis for the search was also lacking in this case. Whereas Belton [was] arrested for drug offenses, Gant was arrested for driving with a suspended license — an offense for which police could not expect to find evidence in the passenger compartment of Gant’s car. Because police could not reasonably have believed either that Gant could have accessed his car at the time of the search or that evidence of the offense for which he was arrested might have been found therein, the search in this case was unreasonable.

Police may search a vehicle incident to a recent occupant’s arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest. When these justifications are absent, a search of an arrestee’s vehicle will be unreasonable unless police obtain a warrant or show that another exception to the warrant requirement applies.

**QUESTIONS**

1. What ramifications do these new rules have on a search incident to arrest for digital evidence devices found in vehicles, such as cell phones, GPS devices, or laptops?

2. What if the driver, who is arrested, has a cell phone in his pocket, a laptop in the front passenger seat, and a GPS device in his vehicle’s dashboard?

3. Can hard drives, which are typically used to store music to play on the vehicle’s sound system, be searched? What about vehicle “black boxes,” that is, event recorders, which register many of the operations of the vehicle, including speed, braking, and air bag deployment?
N. Patrick Crooks, J.

The defendant, Jermichael James Carroll, was charged with possession of a firearm by a felon [and subsequently convicted. The sole basis for that charge was an image that Carroll stored in his cellphone. The question before the court was whether the police legally obtained that image].

Detective Belsha of the Milwaukee police department and his partner were conducting surveillance on a residence as part of an armed robbery investigation. They observed a white Ford Escort leave that residence, slow down as it passed their squad car, and speed away.

The officers attempted to catch the vehicle, which reached speeds of 60 miles per hour on residential streets with speed limits no higher than 25 miles per hour. According to Belsha's testimony, the driver, Carroll, eventually pulled the car to "an abrupt stop" in a gas station lot and quickly got out of the car while holding an object in his hands. The officers could not identify what Carroll was holding, so Belsha drew his weapon and ordered Carroll to drop the object and get on the ground, which Carroll did. The officers then handcuffed Carroll behind his back.

After handcuffing Carroll, Belsha retrieved the dropped object, which was a flip-style cell phone. The cell phone was lying open on the ground and displayed an image of Carroll smoking a long, thin, brown cigarlike object ("the marijuana image"). Belsha, a member of the High Intensity Drug Trafficking Area Drug and Gang Task Force, testified that he recognized the object as a marijuana blunt.

When the officers asked Carroll for identification, Carroll did not have any with him but gave the officers his name. The officers ran a "routine check" and learned that he was driving with a suspended license. Carroll also had a record of being adjudicated delinquent for a drug-related felony two years earlier as a juvenile.

Belsha placed Carroll in the back seat of the squad car and sat in the front seat with the cell phone, where he activated the menus, opened the image gallery, scrolled through it, and saw images showing illegal drugs, firearms, and large amounts of U.S. currency. Specifically, Belsha testified that he saw an image of Carroll with what appeared to be a gallon-size bag of marijuana held in his teeth, and "several photos depicting firearms," including one showing Carroll holding a semiautomatic firearm ("the firearm image").

While Belsha continued to possess Carroll's cell phone, it rang several times and Belsha answered one of those calls, pretending to be Carroll. The caller asked for "four of those things; four and a split." Based on his training, Belsha recognized
that the caller was attempting to purchase four and a half ounces of cocaine.

Two days later, Belsha sought a search warrant for the cell phone. After obtaining the warrant, the police downloaded the data on the cell phone, including the firearm image. Detective McQuown, who was trained in the handling of digital evidence, testified at a preliminary hearing that each image on the phone had attached “metadata,” which he described as information indicating the date and time at which the image was created. He also testified that the metadata is based on the date and time updates regularly provided through cell phone towers. The metadata indicated that the firearm image had been created on May 22, 2006. Carroll was charged with possession of a firearm by a felon based on photographic evidence downloaded from the cell phone.

A. Constitutional Permissibility of the Warrantless Searches

1. Belsha’s Initial Seizure of the Cell Phone

Carroll led officers on a high-speed chase in a car that the officers had been observing in connection with an armed robbery investigation, and exited his car quickly while holding an unknown object. Given that behavior, the officers would have been justified — based on the objective belief that Carroll could have been holding a weapon — in conducting a frisk or pat-down, which would have resulted in Belsha’s legal possession of the cell phone. Hence, Belsha’s order for Carroll to drop the object and his subsequent retrieval of it were reasonable actions, and accordingly, his initial seizure of the phone was justified.

After Belsha legally seized the open phone, his viewing of the marijuana image also was legitimate because that image was in plain view. Under Wisconsin case law, a warrantless seizure is justified under the plain view doctrine where the object is in plain view of an officer lawfully in a position to see it, the officer’s discovery is inadvertent, and the seized object, either in itself or in context with facts known to the officer at the time of the seizure, supplies probable cause to believe that the object is connected to or used for criminal activity.

Here, Belsha was in legal possession of the phone and thus in a lawful position to view the display screen, which, according to Belsha’s uncontroversial testimony, was open and displayed the marijuana image. Further, Belsha testified that based on his experience, he recognized the object Carroll was smoking in the image as a marijuana blunt. That, taken in context with other facts known to Belsha at the time, namely, that individuals involved in drug trafficking often personalize their phones with such images, provided sufficient probable cause to believe that the phone was an instrument of criminal activity and contained evidence linked to that activity. Under the circumstances, Belsha had probable cause to seize the cell phone.

2. Belsha’s Continued Possession of the Cell Phone

After Belsha seized the phone with the marijuana image displayed, he continued to maintain possession of the phone after he had placed Carroll in the squad car. We
conclude that that continued possession was justified. The Court in *United States v. Place*, 462 U.S. 696 (1983), addressed the ability of law enforcement agents to seize and detain a person's luggage based on reasonable suspicion that the luggage contained narcotics and under circumstances where that owner was not in custody or under arrest. The Court went on to hold that the agents had narrow authority to detain temporarily a container in such circumstances though the agents in that case exceeded their authority to do so. However, in reaching its conclusion, the Court explained,

Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the [Fourth] Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present.

In other words, law enforcement agents are justified in seizing and continuing to hold a container if (1) there is probable cause to believe that it contains evidence of a crime, and (2) if exigencies of the circumstances demand it.

Although the “containers” discussed in *Place* were pieces of luggage, it is reasonable to analogize the cell phone in this case to the luggage in *Place*. The underlying concern with the agents’ detention of the luggage in *Place* was that Place had a reasonable expectation of privacy in the contents of his bags. So, too, here, the concern is protecting a person’s reasonable expectation of privacy in the contents of his or her cell phone. Other courts, in assessing the validity of a search without a warrant, have likened a person’s privacy expectations in cell phones and electronic devices to that of closed containers in his or her possession. Accordingly, in this situation, the analogy to a closed container appears to be appropriate.

To establish probable cause to search, the evidence must indicate a “fair probability” that the particular place contains evidence of a crime. An officer’s knowledge, training, and experience are germane to the court’s assessment of probable cause.

Here, Belsha legally viewed the marijuana image; we consider that fact along with his testimony that he knew, based on his training and experience, that drug traffickers frequently personalize their cell phones with images of themselves with items acquired through drug activity. Furthermore, it is those personalized cell phones on which drug traffickers commonly make many of their transactions. We are satisfied, under all of the circumstances here, that that information, taken as a whole, gave Belsha probable cause to believe that the phone contained evidence of illegal drug activity.

Given that Belsha had probable cause to believe that a search of the phone would produce evidence of illegal drug activity, his continued possession of the phone while he sought a warrant was permissible. The same reasons that permitted Belsha to seize the phone in the first instance permitted him to continue to possess it in the short time after Carroll was secured. Exigent circumstances further justify that continued possession. Had Belsha returned the phone to Carroll and released him, Carroll could have deleted incriminating images and data, such as phone numbers and calling records stored in the phone.
3. Belsha’s Browsing Through the Image Gallery and Answering the Incoming Call

Next, two things happened as Belsha continued to possess the phone legally. First, he opened and browsed through the cell phone’s image gallery. Second, he answered an incoming call. As an initial matter, the image gallery search clearly seems to be contrary to the holding in *Place* because there were no exigent circumstances at the time requiring him to review the gallery or other data stored in the phone. We are satisfied that that search was indeed improper and that the evidence obtained from that search at that time was tainted.

However, Belsha’s answering the incoming call was justified. We again apply the standard from *Place*, which requires that the officer had probable cause to believe that the device contains evidence of a crime and that exigent circumstances justify a warrantless search. Here, Belsha had probable cause to believe that the cell phone was a tool used in drug trafficking based on the plain view of the marijuana image and his knowledge that such images are typically found on drug traffickers’ phones. That evidence shows more than a fair probability that an incoming call to such a phone would contain evidence of illegal drug activity.

Moreover, exigent circumstances permitted Belsha’s answering the call. The test for whether exigent circumstances are present focuses on whether the officer reasonably believes that the delay necessary to obtain a warrant, under the circumstances, threatens the destruction of evidence. Several federal cases address whether an officer may, based on exigent circumstances, access data or answer incoming calls on an electronic device that the officer had legally seized.

In the foundational case, *United States v. Ortiz*, [84 F.3d 977 (7th Cir. 1996),] officers seized an electronic pager incident to Ortiz’s arrest for distribution of heroin. While continuing to search Ortiz and his vehicle for evidence, one of the agents pushed a button on the pager that revealed the numeric codes that the pager previously had received. The district court denied Ortiz’s motion to suppress that evidence. The Seventh Circuit Court of Appeals affirmed that denial based on the risk that the data would be destroyed or lost if agents were required to first obtain a warrant:

> Because of the finite nature of a pager’s electronic memory, incoming pages may destroy currently stored telephone numbers in a pager’s memory. . . . Thus, it is imperative that law enforcement officers have the authority to immediately “search” or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence.

In subsequent cases, other courts have adopted that rationale when evaluating an officer’s ability to search a seized cell phone incident to arrest, and have permitted law enforcement to conduct a warrantless search of a phone’s stored data, such as records of calls received and made, so long as the other requirements of the search incident to arrest exception were satisfied.

To be sure, cell phones and pagers are not interchangeable. Indeed, the court in *United States v. Wall*, 2008 U.S. Dist. LEXIS 103058 (S.D.Fla.2008), observed that while exigent circumstances could justify a warrantless search of a cell phone,
[t]he differences in technology between pagers and cell phones cut to the heart of this issue [of whether an officer’s reading of stored text messages within a cell phone was justified based on exigent circumstances]. The technological developments that have occurred in the last decade, since Ortiz was decided, are significant. Previously, there was legitimate concern that by waiting minutes or even seconds to check the numbers stored inside a pager an officer ran the risk that another page may come in and destroy the oldest number being stored. This was based on a platform of first-in-first-out storage of numbers used for pagers. Text messages on cell phones are not stored in the same manner . . . . [I]f a text message is not deleted by the user, the phone will store it.

In Wall, the court concluded that the government failed to demonstrate an exigency justifying the agent’s search of the defendant’s text messages. There, the government put forth no evidence of the danger of the text messages being destroyed; to the contrary, it acknowledged that such messages generally remain stored in the phone unless a user actively deletes them. Given that, the court concluded that the officers’ review of the text messages was purely investigatory and evidence obtained from that review was therefore tainted.

Significantly, at least one court has concluded that when a government agent lawfully possesses a phone and there is probable cause to believe it is used in illegal drug activity, the agent can answer incoming calls if the calls arrive in a period when it is impracticable for the agent to obtain a warrant first. See United States v. De La Paz, 43 F.Supp.2d 370, 375 (S.D.N.Y.1999). In De La Paz, agents had lawfully seized a cell phone incident to an arrest. While the agents were processing the defendant’s arrest, the defendant’s phone rang nine times and the agents answered it each time. The court concluded that it was reasonable under the circumstances for the agents to answer the cell phone of a suspected drug dealer in the time between the arrest and arraignment, given both the impossibility of timely obtaining a warrant allowing agents to answer incoming calls and the risk of losing evidence by leaving those calls unanswered.

The consistent approach taken in these cases is that the courts scrutinized the nature of the evidence obtained, i.e., numeric codes on a pager, stored text messages, and incoming phone calls, and balanced that with an inquiry into whether the agent reasonably believed that the situation required a search to avoid lost evidence. Based on that assessment, it appears that the courts then reserved the exigent circumstances exception for searches directed at the type of evidence that is truly in danger of being lost or destroyed if not immediately seized.

Hence, we are satisfied that exigent circumstances justified Belsha’s answering Carroll’s cell phone. The fleeting nature of a phone call is apparent; if it is not picked up, the opportunity to gather evidence is likely to be lost, as there is no guarantee — or likelihood — that the caller would leave a voice mail or otherwise preserve the evidence. Given these narrow circumstances, Belsha had a reasonable belief that he was in danger of losing potential evidence if he ignored the call. Thus, the evidence obtained as a result of answering that phone call was untainted.
B. Independent Source Doctrine

Having determined that the warrantless seizure and subsequent viewing of the image gallery on Carroll's phone produced tainted evidence, we turn our attention to the question of whether the resulting warrant is nonetheless valid. We conclude . . . that the phone call Belsha answered is an untainted independent source of evidence to support the search warrant, that the untainted evidence, which is combined with the officer's knowledge of drug traffickers and Carroll's juvenile record, provides sufficient probable cause to issue the warrant, and that as a result, the warrant is valid. [Based on the warrant, the search that resulted in the recovery of the firearm image was valid.]

NOTES

1. Exigent Circumstances. In State v. Smith, 920 N.E.2d 949 (Ohio 2009), reproduced supra, the court rejected the legality of a search of a cell phone incident to arrest. The state also argued that the search of the cell phone was proper based on exigent circumstances, that is, “that cell phones store a finite number of calls in their memory and that once these records have been deleted, they cannot be recovered.” The court concluded that the issue was not properly before it, reasoning:

At the suppression hearing, the state offered no evidence or argument to support its claim that the search was justified by the need to preserve evidence. Additionally, even if one accepts the premise that the call records on Smith’s phone were subject to imminent permanent deletion, the state failed to show that it would be unable to obtain call records from the cell phone service provider, which might possibly maintain such records as part of its normal operating procedures.

Based on Smith, what advice would you give to police officers who are validly in possession of a ringing cell phone?