In the
United States Court of Appeals
For the Seventh Circuit

No. 10-3803

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ABEL FLORES-LOPEZ,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of Indiana, Indianapolis Division.
No. 1:09-cr-00136-WTL-KPF-2—**William T. Lawrence**, *Judge*.

ARGUED JANUARY 25, 2012—DECIDED FEBRUARY 29, 2012

Before BAUER, POSNER, and ROVNER, *Circuit Judges*.

POSNER, *Circuit Judge*. This appeal requires us to consider the circumstances in which the search of a cell phone is permitted by the Fourth Amendment even if the search is not authorized by a warrant. Lurking behind this issue is the question whether and when a laptop or desktop computer, tablet, or other type of computer (whether called a "computer" or not) can be searched without a warrant—for a modern cell phone *is* a computer.

Law enforcement authorities had reason to believe that the defendant was a supplier of illegal drugs to another drug dealer, Alberto Santana-Cabrera, who in turn had a retail customer who unbeknownst to him was a paid police informant. The informant, after ordering a pound of methamphetamine from Santana-Cabrera (a large quantity—the informant's hope was that it would induce Santana-Cabrera's supplier to attend the sale, thus enabling the police to land a bigger fish), overheard a phone conversation between Santana-Cabrera and the defendant in which the latter said he would deliver the meth that had been ordered to a garage, where the sale would take place. The police were listening in on the conversation remotely and arrested Santana-Cabrera in the garage and the defendant in front of it.

The defendant had driven a truck containing the meth to the garage, and together with Santana-Cabrera had carried the meth into the garage to await a fourth person (actually an undercover agent), who was to bring the cash for the deal. Upon arresting the defendant and Santana-Cabrera, officers searched the defendant and his truck and seized a cell phone from the defendant's person and two other cell phones from the truck. The defendant admitted that the cell phone found on his person was his but denied that the other cell phones were.

He was tried together with Santana-Cabrera and both were convicted of drug and related offenses. The defendant was sentenced to 10 years in prison. Their appeals were consolidated, but we are deciding Santana-Cabrera's appeal in a separate order, also issued today.

At the scene of the drug sale and arrests, an officer searched each cell phone for its telephone number, which the government later used to subpoena three months of each cell phone's call history from the telephone company. At trial the government sought to introduce the call history into evidence. The history included the defendant's overheard phone conversation with Santana-Cabrera along with many other calls between the defendant and his coconspirators. After a brief hearing the judge overruled the defendant's objection, which however was limited to the call history of the cell phone that he admitted was his, since he denied owning or having used the other cell phones.

The defendant argues that the search of his cell phone was unreasonable because not conducted pursuant to a warrant. The phone number itself was not incriminating evidence, but it enabled the government to obtain such evidence from the phone company, and that evidence, the defendant argues, was the fruit of an illegal search and was therefore inadmissible.

Building on the definition in *New York v. Belton*, 453 U.S. 454, 460 n. 4 (1981), of a container as "any object capable of holding another object," the government responds, with support in case law, see, e.g., *United States v. Murphy*, 552 F.3d 405, 410-12 (4th Cir. 2009); *United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007); cf. *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (pager); *United States v. Thomas*, 114 F.3d 403, 404 n. 2 (3d Cir. 1997) (dictum) (same); but see *State v. Smith*, 920 N.E.2d 949, 953-54 (Ohio 2009), that any

object that can contain anything else, including data, is a container. A diary is a container—and not only of pages between which a razor blade or a sheet of LSD could be concealed, a possibility that justifies the police in turning each page. It is also a container of information, as is a cell phone or other computer. And since a container found on the person of someone who is arrested may be searched as an incident to the arrest even if the arresting officers don't suspect that the container holds a weapon or contraband, and thus without any justification specific to that container, *United States v. Robinson*, 414 U.S. 218, 236 (1973), the government urges that a cell phone seized as an incident to an arrest can likewise be freely searched.

This is a fair literal reading of the *Robinson* decision. But the Court did not reject the possibility of categorical limits to the rule laid down in it. Suppose the police stop a suspected drug dealer and find a diary, but a quick look reveals that it is a personal diary rather than a record of drug transactions, yet the officers keep on reading. A court might say that acquiring information *known* to be unrelated to the crime of which the person being arrested is suspected is an intrusion beyond the scope of *Robinson*'s rule.

A modern cell phone is in one aspect a diary writ large. Even when used primarily for business it is quite likely to contain, or provide ready access to, a vast body of personal data. The potential invasion of privacy in a search of a cell phone is greater than in a search of a "container" in a conventional sense even when the con-

ventional container is a purse that contains an address book (itself a container) and photos. Judges are becoming aware that a computer (and remember that a modern cell phone is a computer) is not just another purse or address book. "[A]nalogizing computers to other physical objects when applying Fourth Amendment law is not an exact fit because computers hold so much personal and sensitive information touching on many private aspects of life. . . . [T]here is a far greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer." *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011); see also *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999); cf. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175-77 (9th Cir. 2010); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). An iPhone application called iCam allows you to access your home computer's webcam so that you can survey the inside of your home while you're a thousand miles away. "iCam—Webcam Video Streaming," http://itunes.apple.com/us/app/icam-webcam-video-streaming/id296273730?mt=8 (visited Feb. 6, 2012, as were the other web sites that we cite in this opinion). At the touch of a button a cell phone search becomes a house search, and that is not a search of a "container" in any normal sense of that word, though a house contains data.

A complication in this case is that, remarkably, the record does not indicate the brand, model, or year of

the defendant's cell phone, so we do not know how dumb or smart it is. But does that matter? Even the dumbest of modern cell phones gives the user access to large stores of information. For example, the "TracFone Prepaid Cell Phone," sold by Walgreens for $14.99, includes a camera, MMS (multimedia messaging service) picture messaging for sending and receiving photos, video, etc., mobile web access, text messaging, voicemail, call waiting, a voice recorder, and a phonebook that can hold 1000 entries. Walgreens, "TracFone Prepaid Cell Phone," www.walgreens.com/store/c/tracfone-prepaid-cell-phone/ID=prod6046552-product.

Given the modern understanding that a warrant is presumptively required for a search—though actually the text of the Fourth Amendment *limits* searches pursuant to warrants, see references in *United States v. Sims*, 553 F.3d 580, 582-83 (7th Cir. 2009), and requires of searches without a warrant only that they be reasonable, the authority to search a person incident to an arrest, without a warrant, requires justification. The usual justification offered is "the need [of the arresting officers] to disarm and to discover evidence," *United States v. Robinson*, *supra*, 414 U.S. at 235, or, more exactingly, evidence that the defendant or his accomplices might destroy, discard, or conceal. *Chimel v. California,* 395 U.S. 752, 763 (1969). The restrictions on searching without a warrant are relaxed when police arrest the driver or passenger of a moving vehicle. They can search the passenger compartment even if they have no reason to think they'll find any evidence, provided that "the arrestee is unsecured and within reaching distance of

the passenger compartment at the time of the search." *Arizona v. Gant*, 129 S. Ct. 1710, 1719 (2009). But in this case the arrest, and the search of the cell phone found on the defendant's person, took place after he had parked and left his vehicle, and so any special rules applicable to searches when police stop a vehicle and arrest an occupant are inapplicable.

In some cases, a search of a cell phone, though not authorized by a warrant, is justified by police officers' reasonable concerns for their safety. One can buy a stun gun that looks like a cell phone. Best Stun Gun, "Cell Phone Stun Guns—Security Products in Disguise," www.beststungun.com/cell-phone-stun-gun.html; Safety Products Unlimited, "The Cell Phone Stun Gun," www.safetyproductsunlimited.com/cell_phone_stun_gun.html. But the defendant's cell phone, once securely in the hands of an arresting officer, endangered no one. It did, however, contain evidence or leads to evidence—as the officers knew was likely because they knew from their informant that as is typical of drug dealers the defendant had used cell phones to talk to Santana-Cabrera and other coconspirators.

But was there any *urgency* about searching the cell phone for its phone number? Yet even if there wasn't, that bit of information might be so trivial that its seizure would not infringe the Fourth Amendment. In *United States v. Concepcion*, 942 F.2d 1170, 1172-73 (7th Cir. 1991), police officers tested the keys of a person they had arrested on various locks to discover which door gave ingress to his residence, and this we said was a

search—and any doubts on that score have been scotched by *United States v. Jones*, 132 S. Ct. 945, 949 (2011), which holds that attaching a GPS device to a vehicle is a search because "the Government physically occupied private property for the purpose of obtaining information." But we went on to hold in *Concepcion* that a minimally invasive search may be lawful in the absence of a warrant, even if the usual reasons for excusing the failure to obtain a warrant are absent, a holding that is implied by *Robinson* and survives *Jones*, which declined to decide whether the search entailed in attaching a GPS device requires a warrant. *Id*. at 954.

So opening the diary found on the suspect whom the police have arrested, to verify his name and address and discover whether the diary contains information relevant to the crime for which he has been arrested, clearly is permissible; and what happened in this case was similar but even less intrusive, since a cell phone's phone number can be found without searching the phone's contents, unless the phone is password-protected—and on some cell phones even if it is. On an iPhone without password protection two steps are required to get the number: touching the "settings" icon and then the "phone" icon. On a Blackberry only one step is required: touching the "phone" icon. Moreover, the phone company knows a phone's number as soon as the call is connected to the telephone network; and obtaining that information from the phone company isn't a search because by subscribing to the telephone service the user of the phone is deemed to surrender

any privacy interest he may have had in his phone number. *Smith v. Maryland*, 442 U.S. 735, 742-43 (1979).

We are quite a distance from the use of the iCam to view what is happening in the bedroom of the owner of the seized cell phone.

It's not even clear that we need a rule of law specific to cell phones or other computers. If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number. If allowed to leaf through a pocket address book, as they are, *United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993), they should be entitled to read the address book in a cell phone. If forbidden to peruse love letters recognized as such found wedged between the pages of the address book, they should be forbidden to read love letters in the files of a cell phone. There is an analogy (implied in *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010), and cases discussed there) to the requirement that wiretaps "minimize the interception of communications not otherwise subject to interception." 18 U.S.C. § 2518(5); *Scott v. United States*, 436 U.S. 128, 130-43 (1978); *United States v. Mansoori*, 304 F.3d 635, 645-49 (7th Cir. 2002).

But set all this to one side and assume that justification is required for police who have no warrant to look inside a cell phone even if all they're looking for and all they find is the phone number. The government emphasizes the danger of "remote wiping." Instant wiping, called "local wiping," as by pressing a button on the cell phone that wipes its contents and at the same time sends an emergency alert to a person previously

specified, see, e.g., Andrew Quinn, "U.S. Develops 'Panic Button' for Democracy Activists," Mar. 25, 2011, www.reuters.com/article/2011/03/25/us-rights-usa-technology-idUSTRE72O6DH20110325; BlackBerry, "Set Maximum Password Attempts IT Policy Rule," http://docs.blackberry.com/en/admin/deliverables/4222/Set_Maximum_Password_Attempts_204136_11.jsp, was not a danger in this case once the officers seized the cell phone. But remote-wiping capability is available on all major cell-phone platforms; if the phone's manufacturer doesn't offer it, it can be bought from a mobile-security company. See, e.g., "Find My iPhone," www.apple.com/iphone/built-in-apps/find-my-iphone.html; "McAfee Mobile Security for Android," www.mcafeemobilesecurity.com; "Kaspersky Mobile Security 9," http://usa.kaspersky.com/products-services/home-computer-security/mobile-security. Wiped data may be recoverable in a laboratory, but that involves delay.

According to Apple, a person with a "jailbroken" iPhone (that is, a "self-hacked" iPhone, modified by its owner to enlarge its functionality or run unauthorized applications) could enable anonymous phone calls to be made, a capability that Apple claims "would be desirable to drug dealers." David Kravets, "iPhone Jailbreaking Could Crash Cellphone Towers, Apple Claims," *Wired*, July 28, 2009, www.wired.com/threatlevel/2009/07/jailbreak/. Apple would like the "jailbreaking" of its phones made illegal, so it is not a disinterested commentator on the use of its phones by those dealers. See, e.g., Adam Cohen, "The iPhone Jailbreak: A Win against Copyright Creep," *Time U.S.*, July 28, 2010, www.time.com/time/nation/article/0,8599,2006956,00.html.

Other conspirators were involved in the distribution of methamphetamine besides Santana-Cabrera and the defendant, and conceivably could have learned of the arrests (they might even have been monitoring the transaction with the informant in the garage from afar) and wiped the cell phones remotely before the government could obtain and execute a warrant and conduct a search pursuant to it for the cell phone's number; and conceivably the defendant might have had time to warn them before the cell phone was taken from him, giving them time to wipe it. "Conceivably" is not "probably"; but set off against the modest benefit to law enforcement of being able to obtain the cell phone's phone number immediately was only a modest cost in invasion of privacy. Armed with that number the officers could obtain the call history at their leisure, and the defendant does not deny that if the number was lawfully obtained the subpoenaing of the call history from the phone company was also lawful and the history thus obtained could therefore properly be used in evidence against him.

The defendant argues that the officers could have eliminated any possibility of remote wiping just by turning off the cell phone. Without power a cell phone won't be connected to the phone network and so remote wiping will be impossible. See, e.g., T-Mobile, "Mobile Security FAQs," http://support.t-mobile.com/docs/DOC-1852; "MobileMe: Troubleshooting, Find My iPhone," http://support.apple.com/kb/TS2734. But a "roving bug" installed in the phone could record everything that the phone's microphone could pick up even though the phone was turned off (because "turning off" a cell

phone often just means a reduction in power—a kind of electronic hibernation). *United States v. Tomero*, 471 F. Supp. 2d 448, 450 and n. 2 (S.D.N.Y. 2007); Nicole Perlroth, "Traveling Light in a Time of Digital Thievery," *New York Times*, Feb. 11, 2012, p. A1, www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html; Vic Walter & Krista Kjellman, "Can You Hear Me Now?," *ABC News*, Dec. 5, 2006, http://abcnews.go.com/blogs/headlines/2006/12/can_you_hear_me/. What we said in *Ortiz* about pagers is broadly applicable to cell phones: "The contents of some pagers also can be destroyed merely by turning off the power or touching a button. See, e.g., *United States v. Meriwether,* 917 F.2d 955, 957 (6th Cir. 1990). 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." *United States v. Ortiz*, *supra*, 84 F.3d at 984.

And if the phone is either turned off or powered down to a level at which it appears to be turned off, the police can't obtain information from it, even its phone number, knowledge of which as we said is minimally invasive of privacy. The alternative to searching the cell phone forthwith or turning it off (*really* turning it off—not just powering it down) is to place it in a "Faraday bag" or "Faraday cage" (essentially an aluminum-foil wrap) or some equivalent, which isolates the cell phone from the phone network and from Bluetooth and wireless Internet signals. See, e.g., Department of Justice, Computer Crime and Intellectual Property Section, "Awareness Brief: Find

My iPhone" (June 18, 2009); Cindy Murphy, "Cellular Phone Evidence: Data Extraction and Documentation," http://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf. (Faraday bags or cages are found in consumer products such as microwave ovens to keep the microwaves in, and in coaxial cables to keep interfering radio signals out.) It is also possible to "mirror" (copy) the entire cell phone contents, to preserve them should the phone be remotely wiped, without looking at the copy unless the original disappears. See Keir Thomas, "Is Smartphone Security Good Enough?," *PCWorld*, Apr. 20, 2011, www.pcworld.com/businesscenter/article/225771/is_smartphone_security_good_enough.html; American Civil Liberties Union of Michigan, "ACLU Seeks Records about State Police Searches of Cellphones," Apr. 13, 2011, www.aclumich.org/issues/privacy-and-technology/2011-04/1542; Cellebrite, "UFED Ultimate," www.cellebrite.com/ mobile-forensics-products/forensics-products/ufed-ultimate.html.

We said it was conceivable, not probable, that a confederate of the defendant would have wiped the data from the defendant's cell phone before the government could obtain a search warrant; and it could be argued that the risk of destruction of evidence was indeed so slight as to be outweighed by the invasion of privacy from the search. But the "invasion," limited as it was to the cell phone's number, was also slight. And in deciding whether a search is properly incident to an arrest and therefore does not require a warrant, the courts do not conduct a cost-benefit analysis, with

the invasion of privacy on the cost side and the risk of destruction of evidence (or of an assault on the arresting officers) on the benefit side of allowing the immediate search. Toting up costs and benefits is not a feasible undertaking to require of police officers conducting a search incident to an arrest. Thus, even when the risk either to the police officers or to the existence of the evidence is negligible, the search is allowed, *United States v. Robinson*, *supra*, 414 U.S. at 235, provided it's no more invasive than, say, a frisk, or the search of a conventional container, such as Robinson's cigarette pack, in which heroin was found. If instead of a frisk it's a strip search, the risk to the officers' safety or to the preservation of evidence of crime must be greater to justify the search. *Campbell v. Miller*, 499 F.3d 711, 717 (7th Cir. 2007), citing *Mary Beth G. v. City of Chicago*, 723 F.2d 1263, 1273 (7th Cir. 1983). Looking in a cell phone for just the cell phone's phone number does not exceed what decisions like *Robinson* and *Concepcion* allow.

We need not consider what level of risk to personal safety or to the preservation of evidence would be necessary to justify a more extensive search of a cell phone without a warrant, especially when we factor in the burden on the police of having to traipse about with Faraday bags or mirror-copying technology and having to be instructed in the use of these methods for preventing remote wiping or rendering it ineffectual. We can certainly imagine justifications for a more extensive search. The arrested suspect might have prearranged with coconspirators to call them periodically

and if they didn't hear from him on schedule to take that as a warning that he had been seized, and to scatter. Or if conspirators buy prepaid SIM (subscriber identity module) cards, each of which assigns a different phone number to the cell phone in which the card is inserted, and replace the SIM card each day, a police officer who seizes one of the cell phones will have only a short interval within which to discover the phone numbers of the other conspirators. See Adrian Chen, "The Mercenary Techie Who Troubleshoots for Drug Dealers and Jealous Lovers," *Gawker*, Jan. 25, 2012, http://gawker.com/5878862/. (This is provided the phone number is on the SIM card; in some iPhones, for example, it is not.) The officer who doesn't make a quick search of the cell phone won't find other conspirators' phone numbers that are still in use.

But these are questions for another day, since the police did not search the contents of the defendant's cell phone, but were content to obtain the cell phone's phone number.

AFFIRMED.