Washington Journal of Law, Technology & Arts

Volume 8 | Issue 4 Article 3

2-1-2013

When Is a Phone a Computer?

J. C. Lundberg

Follow this and additional works at: https://digitalcommons.law.uw.edu/wjlta

 Part of the Criminal Procedure Commons

Recommended Citation
J. C. Lundberg, *When Is a Phone a Computer?*, 8 WASH. J. L. TECH. & ARTS 473 (2013).
Available at: https://digitalcommons.law.uw.edu/wjlta/vol8/iss4/3

This Article is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington Journal of Law, Technology & Arts by an authorized editor of UW Law Digital Commons. For more information, please contact lawref@uw.edu.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 4 WINTER 2013

WHEN IS A PHONE A COMPUTER?

J.C. Lundberg[*]
© J.C. Lundberg

Cite as: 8 WASH. J.L. TECH. & ARTS 473 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1227

ABSTRACT

In United States v. Kramer*, the Eighth Circuit upheld a two-level sentence enhancement for a defendant who made calls and sent text messages from a cellphone to a minor in order to lure her across state lines for criminal sexual activity. This enhancement was based on a provision in the United States Sentencing Guidelines that incorporates the definition of "computer" from the Computer Fraud and Abuse Act. The broad language of that statute encompasses not only computers—in the plainest sense—and cellphones, but also a myriad of other devices such as automobiles equipped with GPS navigation. In contrast to the sentencing context, this conception of many electronics devices as "computers" does not extend into issues related to searches. There, courts tend to permit broader examination of cellphones and other electronic devices in searches incident to arrest, despite the general protection computers are usually afforded under the Fourth Amendment.*

---

[*] J.C. Lundberg, University of Washington School of Law, Class of 2013. Many thanks to Lauren Guicheteau, Jane Winn and Peter Winn for all their input on this Article.

TABLE OF CONTENTS

INTRODUCTION

In a recent case, *United States v. Kramer*,[1] the Eighth Circuit held that a two-level sentencing enhancement was appropriate when a defendant used a cellphone to induce a minor to cross state lines for criminal sexual activity. This enhancement applied because Kramer's cellphone was deemed to qualify as a computer under the relevant statutory definition of the Computer Fraud and Abuse Act.[2] This definition is so encompassing that Steve Wozniak's somewhat flippant claim, "[e]verything has a computer in it nowadays,"[3] becomes a troubling reality for many criminal defendants. Given the realities of how this class of crimes is committed and the sweeping definition above, effectively all defendants sentenced for such crimes will be eligible for the sentence enhancement. In contrast, computers—as traditionally conceived—are offered unique protection from searches under the Fourth Amendment. Under searches incident to arrest and those pursuant to a warrant, computer searches must be narrowly tailored. This double reading of the word "computer"—expansive for sentencing purposes and narrow for Fourth Amendment purposes—reflects the fog which plagues courts trying to apply

---

[1] 631 F.3d 900 (8th Cir. 2011).

[2] 18 U.S.C. § 1030 (e)(1) (2006).

[3] Mark Millian, *Apple's Steve Wozniak: 'We've lost a lot of control'*, CNN TECH (Dec. 8, 2010, 12:16 PM), http://articles.cnn.com/2010-12-08/tech/steve.wozniak.computers_1_computer-whiz-computer-history-museum-apple-shares?_s=PM:TECH.

traditional principles or older statutes to our rapidly evolving technology.

I. THE WORD "COMPUTER" AND SENTENCING

A common dictionary definition of "computer" is any "device that computes, especially a programmable electronic machine that performs high-speed mathematical or logical operations or that assembles, stores, correlates, or otherwise processes information."[4] This definition encompasses essentially all portable electronics—including iPods, smartphones, e-readers and iPads—as well as many microwaves and televisions. However, in common usage, "computer" generally intends either a laptop or desktop PC. Generally, most people think a computer is a device with a full QWERTY keyboard designed to be typed on at length.[5] Considering a more expansive definition than the intuitive one outlined above, the borders of where a modern device stops being a computer in any meaningful sense of the word is when a user cannot use the device to connect to the Internet.

The United States Sentencing Guidelines (USSG) include an enhancement of two levels if the "offense involved the use of a computer . . . to (A) persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct; or (B) entice, encourage, offer, or solicit a person to engage in prohibited sexual conduct with the minor."[6] The U.S. Sentencing

---

[4] AMERICAN HERITAGE DICTIONARY.

[5] The increasing adoption of tablet devices, including the iPad and Microsoft Surface, shows some of the difficulty in defining "computer" in a way that is acceptable everyone. Some call these products halfway between a laptop and a smartphone. Michael Arrington, *The Unauthorized TechCrunch iPad Review*, TECHCRUNCH (Apr. 2, 2010), http://techcrunch.com (calling the iPad a "New category of device"). Others deride them as oversized smartphones. Matthew Shaer, *iPad nothing more than an oversized Apple iPhone: Motorola*, THE CHRISTIAN SCIENCE MONITOR: HORIZONS (Dec. 21, 2010), http://www.csmonitor.com/Innovation/Horizons.

[6] United States Sentencing Guidelines § 2G1.3 (b)(3) (2013). Similar enhancements—albeit not always with identical language—appear in USSG §§ 2A3.1 ("Criminal Sexual Abuse" or Attempt), 2A3.2 (Statutory Rape or Attempt), 2A3.3 ("Criminal Sexual Abuse of a Ward" or Attempt), 2A3.4 ("Abusive Sexual Contact" or Attempt), 2G2.1 (Creation of Child Pornography),

Guidelines incorporate the definition of "computer" in the Computer Fraud and Abuse Act (CFAA). "'Computer' has the meaning given that term in 18 U.S.C. § 1030(e)(1)."[7] In turn,

> the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.[8]

A cellphone is not a typewriter, calculator, or similar device. The deciding factor in the CFAA analysis has to do with the storage capacity. Some typewriters have a one line memory and most four function calculators can remember a single number but beyond that they rely on the user to supply data and processing power. Even the most rudimentary cellphone available on the market today qualifies as a computer under the CFAA due to its ability to, at a minimum, store a call history and list of contacts. The Seventh Circuit adopted this reasoning and spoke in even broader terms, stating that "[e]very cell phone and cell tower is a 'computer' under this statute's definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget."[9] One commentator expands on the category of "many another gadget [sic]" which "can include coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers."[10]

2G2.2 (Trafficking in Child Pornography), 2G2.6 ("Child Exploitation Enterprises"), 2G3.1 ("Importing, Mailing, or Transporting Obscene Matter"), and 2H3.1 ("Interception of Communications").

[7] United States Sentencing Guidelines § 2G1.3 (2012), Note 1, Definitions.

[8] 18 U.S.C. § 1030 (e)(1).

[9] U.S. v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005).

[10] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577-1578 (2010) (footnote omitted).

As a practical matter, there is a question of how some of the broader instances above could actually trigger the USSG computer-use enhancement. How, for example, could a coffeemaker be used to lure a child across state lines for immoral purposes? Some hypotheticals, however, are not so farfetched. One not addressed in any published case thus far would be the use of a modern automobile to transport a minor across state lines, absent the use of any other computer. The myriad of computerized controls, not to mention built-in GPS devices, inherent in a newer vehicle renders it a "computer" under the CFAA. As such, the individual who used such a car to transport a child across state lines for immoral purposes could be subject to the 2-level enhancement of USSG § 2G1.3 (b)(3) as was the defendant in *Kramer*. If an attempt were made by a U.S. Attorney to seek the enhancement, the intuitive understanding that cars and computers differ significantly, is likely to prevail, causing the enhancement to be denied.

II. COMPUTERS AND THE FOURTH AMENDMENT

There are two general streams of jurisprudence addressing searches: searches pursuant to a warrant and searches incident to arrest. The latter—searches performed in the context of an arrest—generally offer far less protection for suspects than the former. In both situations, however, computers are treated very differently from cell phones and similar devices.

A. Warrant Searches

The general rule governing searches is that a search of a person's effects or papers requires a warrant.[11] The Fourth Amendment requires that warrants are written "particularly describing the place to be searched, and the persons or things to be seized."[12] This protection ensures that warrant searches are strictly limited to the scope of the warrant, even going so far to limit what

---

[11] *See generally* U.S. CONST. amend. IV.
[12] *Id.*

sort of data the police can search for on a computer.

Some courts attempt to resolve the limits of warrant computer searches by utilizing traditional ideas in Fourth Amendment law, especially the closed container doctrine, which prohibits warrantless searches of a closed container.[13]

In applying these traditional ideas to computers, a prosecutor in the case *U.S. v. Crist* argued that a defendant's entire computer should be treated as a single closed container. The Middle District of Pennsylvania did not accept the U.S. Attorney's reasoning. "A hard drive is not analogous to an individual disk. Rather, a hard drive is comprised of many platters, or magnetic data storage units, mounted together. Each platter, as opposed to the hard drive in its entirety, is analogous to a single disk as discussed in *Runyan*."[14] The court relied on the technical aspects of hard drive construction, which offered an avenue of limiting the search.

With advents in data storage technology, however, this limit will do little good going forward. The storage on many newer computers, and on all cellphones, is flash-based rather than platter-based.[15] While similar reasoning may be applied—multiple chips in a flash hard drive and multiple platters in a traditional hard drive—some smaller devices, like cellphones, use flash chips for their storage. *Crist*'s reasoning could also protect, for example, a car's GPS history information if the warrant is only written to permit searching the interior of the car for specific items or classes of items. For that matter, a warrant authorizing a search for any kind of item—that is, physical object—may not permit any search of the car's computer systems or GPS history since digital data is not an object.[16]

---

[13] See generally U.S. v. Monghur, 588 F.3d 975 (9th Cir. 2009).

[14] U.S. v. Crist, 627 F.Supp.2d 575, 586 (2008, M.D. Penn.) (citing U.S. v. Runyan, 275 F.3d 449 (5th Cir. 2001)).

[15] One example is Apple's Macbook Air which, since 2010, is only available with flash hard drives. As time goes on, the list of potential examples of this kind of storage in laptops grows prodigiously.

[16] Courts addressing GPS data generally do so in the context of tracking units placed on cars by police officers. *See, e.g.*, United States v. Jones, 132 S.Ct 945 (2012). As such, courts have not addressed this information/object distinction directly but it could be leveraged by defendants seeking to exclude some information.

A better rubric under which to analyze warrant searches of computers is offered by *U.S. v. Carey*.[17] In that case, an officer searching a computer came upon an image of child pornography. Instead of stopping for a modification of the warrant, the officer continued to search the computer for child pornography. "The warrant authorized the officer to search any file because 'any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information.'"[18] When the search was challenged, the court found that the first incidence of child pornography was a licit find because it was in digital plain view, but the remainder resulted from the officer's indifference to the warrant. "The Supreme Court has instructed, 'the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.'"[19] Warrant searches must be limited not only to the places the warrant allows but also to the thing to be found.

Despite the use of more traditional categories, including the plain view and closed container doctrines, some courts have attempted to extend general search protections over computers and other electronics. In *United States v. Arnold*, the district court held:

> [T]he information contained in a laptop and in electronic storage devices renders a search of their contents substantially more intrusive than a search of the contents of a lunchbox or other tangible object. A laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records.[20]

---

[17] 172 F.3d 1268 (10th Cir. 1999).

[18] *Id*. at 1272.

[19] *Id*. at 1272 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)).

[20] United States v. Arnold, 454 F.Supp.2d 999, 1003–1004 (C.D.Cal. 2006) reversed by U.S. v. Aronld, 523 F.3d 941 (9th Cir. 2008). The appeal was

The decision in *Arnold* shows that some judges are increasingly aware of the broad sweep permissive electronics searches would make into the private lives of individuals who may well have done nothing wrong.

B. Automobile Exception

Despite the traditional protection against searches of closed containers, cell phones may be "opened" under the automobile exception.[21] The jurisprudence addressing searches of cellphones is generally centered on phones found in automobiles, where longstanding rules permit their search despite the special protection generally afforded to computers. The limits of this exception are drawn by probable cause and "not defined by the nature of the container in which the contraband is secreted. Rather, the exception is defined by the object of the search and the places in which there is probable cause to believe that it may be found."[22]

This automobile exception is similar to the general exception to the privacy right that is triggered when an individual is arrested.

> [T]he police may also examine the contents of any containers found within the passenger compartment, for if the passenger compartment is within reach of the arrestee, so also will containers in it be within his reach. Such a container may, of course, be searched whether it is open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have.[23]

The application of this exception, however, treats cellphones and computers quite differently. While both have been shoehorned into the legal framework of the closed container doctrine, computers

---

decided on the grounds that the search occurred at a border where warrantless searches are widely permitted.

[21] United States v. Ross, 456 U.S. 798 (1982).

[22] *Id.* at 824.

[23] New York v. Belton, 453 U.S. 454, 460–61 (1981) (footnotes omitted).

have been exempted from the automobile exception but cellphones have not.

The Tenth Circuit has explicitly exempted computers from the automobile exception. In *U.S. v. Burgess*,[24] the Court analyzed a search of a defendant's motorhome, which revealed marijuana, cocaine, a laptop, and an external hard drive.[25] In analyzing whether the discovery, and subsequent search, of the computer was licit, the court refused to follow the government's simple "syllogism": (1) the expected privacy of the contents of a computer is like that of a briefcase; (2) the automobile exception permits searches of briefcases, even if locked, found in automobiles given probable cause; hence (3) police may—given probable cause—search computers found in automobiles.[26]

The *Burgess* court did not disagree that the syllogism was formally valid, but clarified that the treatment of computers as closed containers was done "to emphasize the high expectation of privacy for" computers and "not to permit promiscuous searches under the automobile exception."[27] In dicta, the court emphasized that computers hold much information about an individual's life, very little of which would be relevant for criminal investigation. Accordingly, a warrantless search of a computer would be like a warrantless search of "relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site."[28] While officers may seize such papers for evaluation pursuant to a search warrant granted by a magistrate when they cannot feasibly search them on site, "[t]he magistrate should then require officers to specify in a warrant which type of [documents] are sought."[29] Under similar reasoning, computers would be exempted from the automobile exception.[30]

---

[24] 576 F.3d 1078 (10th Cir. 2009).

[25] *Id*. at 1082-83.

[26] *Id*. at 1088 citing California v. Acevedo, 500 U.S. 565, 580 (1991) (confirming the applicability of the automobile exception to locked briefcases).

[27] U.S. v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (quoted in *Burgess*, 576 F.3d at 1089).

[28] *Id.*

[29] *Id.*

[30] The Tenth Circuit ultimately punted on the issue, despite much discussion, because "[i]nteresting as the issue may be, we need not now resolve

Implicit in some courts' dicta is the idea that computers are not subject to the automobile exception. For example the U.S. District Court for the Western District of Missouri ruled, in an unpublished opinion, on a criminal defendant's motion to suppress information found on his cellphone after it was discovered in an automobile search an officer conducted after the defendant's arrest. "The Court concludes that the automobile exception to the Fourth Amendment's warrant requirement gave Officer Hilburn's [sic] latitude to search defendant's cell phone and camera, like it would allow the search of other closed containers in the vehicle."[31] This conclusion was followed immediately by a footnote distinguishing *Kramer*—on which the defendant relied—because it did not consider the Fourth Amendment implications of the computer/cellphone unification.

This double standard has not gone unnoticed by Fourth Amendment scholars. "If current Fourth Amendment jurisprudence is extended to its logical conclusion, officers who arrest drivers for traffic infractions will be permitted to search the call histories, text messages, email, photos, movies, and Internet browsing history on iPhones with no suspicion of wrongdoing whatsoever."[32] In fact, the same line of reasoning would also permit the examination of the history of a GPS device found in, or built into, a car. Because this area of jurisprudence is currently growing and developing, it remains to be seen whether these concerns will come to fruition, but they certainly mark one possible trend of the unfolding interface of the Fourth Amendment and portable technology.

C. Searches Incident to Arrest

Outside the context of automobiles, the permissibility of searches incident to arrest centers on the safety of officers. Because this standard is narrower than the automotive exception, it will be much less likely to cover the search of a cellphone, and its

---

it because the search of Burgess' hard drives was authorized by a warrant." Burgess, 576 F.3d at 1090.

[31] U.S. v. Stringer, 2011 WL 3847026, *9 (W.D. Missouri July 20, 2011).

[32] Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 27 (2008).

bounds generally preclude a search of an arrestee's cellphone's memory.

The Supreme Court has clearly delineated the reasons for warrantless searches incident to arrest. "The exception [to a general requirement for a warrant] derives from interests in officer safety and evidence preservation that are typically implicated in arrest situations."[33] The dangers in both categories are clear. A weapon in an arrestee's control can harm the arresting officer, other officers, or other arrestees, and evidence left in an arrestee's possession can easily be damaged or destroyed before recovered during booking. Neither category offers purchase for a warrantless search of either computers or cellphones conducted incident to arrest.

Courts place extreme importance on the intent of the officer in searches incident to arrest. If the search was conducted for officer safety, the evidence will likely be permitted. In other circumstances, the Northern District of California struck down a search of defendants' cellphones conducted subsequent to arrest because the "[o]fficers did not search the phones out of a concern for officer safety, or to prevent the concealment or destruction of evidence. Instead, the purpose was purely investigatory. Once the officers lawfully seized defendants' cellular phones, officers could have sought a warrant to search the contents of the cellular phones."[34] As a practical matter, it is unlikely that officer safety would ever justify a search of a cellphone's memory.

Similarly, cellphone memory is generally long-lasting and robust, thereby preserving evidence which does not offer sufficient reason to protect a warrantless search of an arrestee's cellphone. In *State v. Smith*[35], the Supreme Court of Ohio rejected a search of a cellphone made subsequent to arrest on the grounds that the Government failed to show that any of its data faced imminent deletion or destruction and that it could not be found any other way.[36] Much like the Supreme Court of Ohio, the Northern District

---

[33] Arizona v. Grant, 556 U.S. 332, 338 (2009).

[34] U.S. v. Park, 2007 WL 1521573, *8 (N.D. California May 23, 2007).

[35] 920 N.E. 2d 949 (Ohio 2009)

[36] See THOMAS K. CLANEY, CYBER CRIME AND DIGITAL EVIDENCE: MATERIALS AND CASES 187 (2011). There are potential situations where

of California placed cellphones outside the reach of warrantless searches incident to arrest; "a cellular phone should not be characterized as an element of individual's clothing or person, but rather as a 'possession[ ] within an arrestee's immediate control [that has] fourth amendment [sic] protection at the station house.'"[37]

CONCLUSION

The word "computer" has a myriad of meanings depending on the context in which it is used. The choice of the meaning has a substantive effect on the legal framework applied to the object in question. In the sentencing context, for example, "computer" has the broad meaning under the Computer Fraud and Abuse Act, which can then result in the use of a simple cellphone rendering a defendant eligible for a sentencing enhancement. On the other hand, sometimes courts look past terminology to the functional aspects of the device in question, often traditional doctrines such as the closed container doctrine. Even in these contexts, however, some courts treat cellphones and computers much differently, typically to a defendant's detriment.

What devices can be searched, in what manner, and when are evolving areas of the law. One can only "speculate whether the Supreme Court would treat laptop computers, hard drives, flash drives or even cell phones as it has a briefcase or give those types of devices preferred status because of their unique ability to hold vast amounts of diverse personal information."[38] In the meantime, the mixed judicial reactions to the evidentiary implications of the word "computer" can offer advantage to both sides in criminal cases.

---

evidence on a cellphone could be destroyed if not investigated at the time of arrest, they are not identifiable ex ante by an officer at the scene. One would be an iPhone that can be remotely wiped by someone with its associated iCloud account password. Determining whether such data will be deleted is impossible to tell before it begins.

[37] U.S. v. Park, 2007 WL 1521573, *8 (N.D. California May 23, 2007) (quoting U.S. v. Monclavo-Cruz, 662 F.2d 1285, 1290 (9th Cir. 1981)).

[38] U.S. v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009).

PRACTICE POINTERS

- Prosecutors: Point to instances where courts have been widely permissive of searches of new technologies, especially cellphones.
- Defenders: Point to the fact that a cellphone or other pieces of new technology often hold as much intimate information about an individual as a computer. They should, therefore, be extended the same protection.