# BIG BROTHER OR LITTLE BROTHER? SURRENDERING SEIZURE PRIVACY FOR THE BENEFITS OF COMMUNICATION TECHNOLOGY

*José Felipé Anderson*[*]



> They that can give up essential liberty to obtain a little temporary safety deserve neither safety nor liberty.[1]
>
> Benjamin Franklin

> O cruel, needless misunderstanding! . . . But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother.[2]
>
> George Orwell

---

* Professor of Law and Founding Director Stephen L. Snyder Center for Litigation Skills (2000-2008) University of Baltimore School of Law. Adjunct Professor of Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania. Research funding for this work was underwritten by the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, which is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs at the U.S. Department of Justice. The author acknowledges Professor Thomas K. Clancy, Director of the National Center for Justice and the Rule of Law, the faculty, panel participants, appellate judges and students of the University of Mississippi School of Law who attended a lecture and discussion of an earlier draft of this paper, and for the many helpful suggestions that resulted.

[1] Benjamin Franklin, *Reply of the Pennsylvania Assembly to the Governor (Nov. 1755)*, *in* POWER QUOTES 106 (Daniel B. Baker ed., 1992).

[2] GEORGE ORWELL, 1984 at 266 (Plume 1983) (1949).

## INTRODUCTION

Over two centuries have passed since Benjamin Franklin quipped that we should defend privacy over security if people wanted either privacy or security.[3] Although his axiom did not become a rule of law in its original form, its principles found voice in the Fourth[4] and Fifth[5] Amendments of the Constitution's Bill of Rights.[6] To a lesser extent, provisions against the quartering of

---

[3] Franklin, *supra* note 1.

[4] The Fourth Amendment of the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. One Fourth Amendment historian has explained that the:

> Amendment provides that if there is to be a search and seizure, it must be a reasonable one. The only absolute standard that is set is as to the essentials of a warrant when such is necessary, as it is in most cases. The purpose of the latter part of the Amendment of course is to safeguard against the general warrant and it does this in two ways: first, by prescribing the requirement of probable cause, necessarily peculiar to each case; and second, by making requisite the description of the particular place to be searched, the persons to be apprehended, and the objects to be seized. These requirements limit the scope of each warrant; they take the decision as to what may and what may not be done out of the hands of the officer who is to execute the warrant, and place it with the more trustworthy and sober judgment of a judicial officer. It is for the latter to pass upon the merits of the allegations and, on the basis of evidence having behind it the responsibility of an oath, to decide whether there is reasonable justification for this exceptional proceeding in invasion of the individual's privacy, and thus to determine what particular actions are justified on the basis of this showing. There is no temptation for the ministerial officer to exceed the authority which the magistrate decides to give him, for he not only thereby subjects himself to civil and criminal liability but gains no advantage over the accused and merely wastes his effort.

NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 120 (1937) (footnote omitted).

[5] U.S. CONST. amend. V.

[6] One Supreme Court Justice has said:

> [T]he concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them

troops in private homes found in the Third Amendment[7] also support the idea that what a government can require you to do, or who you must have behind the doors of your home, is an area of grave importance for privacy purposes.[8] By our behavior as a nation, have we indicated a rejection of the liberty Franklin was writing about in our modern times? In no area has the rapid rise of technology affected our lives more than in the area of communication through computers and other devices, like so-called "smart telephones."[9]

---

> from the pressures of a turbulent life around them and give them health and strength to carry on.

United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting).

[7] "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III.

[8] In *Camara v. Municipal Court*, 387 U.S. 523, 529 (1967), the Supreme Court said:

> The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.

*Id.* (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)) (internal quotation marks omitted). The Fourth Amendment reflects critical values. "Indeed, these rights are so strong that the Constitution prohibits the most minimal transgressions against them. . . . Personal security, liberty, and private property are not discrete interests; they unite to define significant attributes of individual freedom in the democracy." Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 576 (1996).

[9] So-called smart phone technology has made it possible to perform many communications functions in a small device when such tools were unimaginable only a few years ago. The Supreme Court has already demonstrated a willingness to allow technology, such as tracking devices, to evade constitutional scrutiny. *See* United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that placing a beeper type location device, without a warrant, in a barrel of contraband is not a search under the Fourth Amendment). It is unlikely that the Court desires to get involved in the day-to-day regulation of emerging technology. Most recently, the Supreme Court clarified its view on high technology searches in *United States v. Jones*, where it held that the government's use of a Global Positioning System on a private vehicle to monitor its movements constituted a search under the Fourth Amendment, therefore requiring a warrant to be obtained. *See* 132 S. Ct. 945 (2012). The *Jones* case seems curiously in conflict with the Court's prior holding in *Knotts*—invalidating the warrantless search—in that Justice Scalia's opinion pointed out that the "government physically occupied private property for the purpose of obtaining information." *Jones*, 132 S. Ct. 945, 949. Harkening back to the colonial days when horse and carriage was the primary mode of on-road transportation, the Justice reasoned that the intrusion in

As long as people have been communicating, there has been a desire for others to be interested in hearing what they say.[10] Sometimes the speaker or writer desires an audience and the speaker's freedom to communicate desires protection.[11] At other times, people intend to keep their private words private while others desire to know their thoughts and intentions. This human desire, the "right to be let alone,"[12] has both practical and legal

---

*Jones* was no different than "a constable's concealing himself in the target's coach in order to track its movements." *Jones*, 132 S. Ct. at 950 n.3. It remains to be seen whether this opinion signals any movement toward the Supreme Court extending greater privacy from technology-assisted searches. It only hinted in the opinion that it "may eventually have to grapple with these 'vexing problems' in some future cases . . . ." *Jones*, 132 S. Ct. at 954. Currently, such conflicting opinions on intrusion technology when the Supreme Court takes on such cases do not provide ample guidance as technology advances. In my view these occasional rulings on such searches will do little to provide more privacy.

[10] The most familiar area of electronic intrusion that courts have addressed is wiretapping. But such surveillance, that is, listening in secret, is an ancient practice. As one court recently explained:

> Eavesdropping is an ancient practice which at common law was condemned as a nuisance. At one time the eavesdropper listened by naked ear under the eaves of houses or their windows, or beyond their walls seeking out private discourse. The awkwardness and undignified manner of this method as well as its susceptibility to abuse was immediately recognized. Electricity, however, provided a better vehicle and with the advent of the telegraph surreptitious interception of messages began. As early as 1862[,] California found it necessary to prohibit the practice by statute. During the Civil War General J.E.B. Stuart is reputed to have had his own eavesdropper along with him in the field whose job it was to intercept military communications of the opposing forces. . . .
>
> The telephone brought on a new and more modern eavesdropper known as the 'wiretapper.' Interception was made by a connection with a telephone line.

Kopko v. Miller, 842 A.2d 1028, 1034 (Pa. Commw. Ct. 2004) (quoting Berger v. New York, 388 U.S. 41, 45-46 (1967)).

[11] "In time, given the global movement toward democracy, interactive voice, audio, video data exchange will occur world wide. In addition to fiber optics, dozens of other technological innovations will end our dependency on the electromagnetic spectrum." JONATHAN W. EMORD, FREEDOM, TECHNOLOGY AND THE FIRST AMENDMENT 308 (1991).

[12] The right to be let alone by government officials, unless there exists sufficient cause, is protected by the Fourth Amendment. This right is "perhaps the most personal of all legal principles. It is also one of the newest, since only the more sophisticated of societies have the interest and the ability to nurture that subtle and most personal possession of man, his dignity." MORRIS L. ERNST & ALAN U. SCHWARTZ, PRIVACY: THE RIGHT TO BE LET ALONE 1 (1962).

limitations. Obviously society has its own right to protect its members from violence and keep the peace by legislating and enforcing criminal law.[13] When technology comes into existence, law enforcement often uses it first to engage in the "competitive enterprise [to] ferret[] out crime."[14] Further, the technology itself may make it impossible to permit people who desire to keep information private from achieving that goal. Among the reasons that keeping matters private has become more difficult is that the law simply cannot keep up with the rapid rise in communications technology.[15]

The rise in technology is not a new issue;[16] what is new is our willingness to surrender control of how our personal information

---

[13] *See Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 78 (2000) (statement of Kevin V. DiGregory, Deputy Assoc. Att'y Gen. DOJ). "Carnivore is '[e]ssentially a personal computer stuffed with specialized software, [which] represents a new twist in the federal government's fight to sustain its snooping powers in the Internet age.' The *Wall Street Journal* also reported that Carnivore 'can scan millions of e-mails a second' . . . ." Trenton C. Haas, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261, 261 (2001) (alteration in original) (footnote omitted) (quoting Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-mail Spark Concern*, WALL ST. J., July 11, 2000, at A3).

[14] Johnson v. United States, 333 U.S. 10, 14 (1948).

[15] The ability of government to intrude electronically increases each day as technology advances. Without statutory controls, it is likely that fewer areas of our lives can be kept private. One insightful commentator has explained that:

> [E]lectronic surveillance is almost inherently indiscriminate. Interception of a telephone line provides to law enforcement all of the target's communications, whether they are relevant to the investigation or not, raising concerns about compliance with the particularity requirement in the Fourth Amendment and posing the risk of general searches. In addition, electronic surveillance involves an on-going intrusion in a protected sphere, unlike the traditional search warrant, which authorizes only one intrusion, not a series of searches or a continuous surveillance. Officers must execute a traditional search warrant with dispatch, not over a prolonged period of time. If they do not find what they were looking for in a home or office, they must leave promptly and obtain a separate order if they wish to return to search again. Electronic surveillance, in contrast, continues around-the-clock for days or months. Finally, the usefulness of electronic surveillance depends on lack of notice to the suspect.

James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 70 (1997) (footnotes omitted).

[16] Professor Arthur Miller, in a prophetic statement about a quarter of a century ago, framed the challenge of the courts' role in privacy protection and the challenges

is stored and accessed in the face of our desire for the convenience that communications technology offers. It is that topic on which this Article focuses. This commentary is not intended to be an extensive review of any aspect of the debate over privacy and technology. Indeed, my purpose is to make thoughtful people ask questions about how comfortable they have become with the mass of easily accessible personal information stored by so many entities.

These disputes about privacy, like all critical legal disputes unaddressed by the legislature, will find their way to the nation's courts. We can fully expect that the future will bring more disputes into the judicial system as more technology is created, impacting our private information and bringing new meaning to the often-used expression that "Big Brother is watching."[17] One such dispute recently made its way to court in a somewhat unusual way, emerging as a sentencing issue in a child sexual abuse case, rather than a motion to suppress evidence alleged to be illegally seized in a criminal prosecution.[18] In the case of

---

that courts and society would face as we anticipated the promise of the high technology age. He wrote:

> The notion that the courts will recognize a general principle requiring data handlers to treat personal information as confidential or will declare that file keepers owe a fiduciary duty to file subjects seems to be wishful thinking. Nor is it realistic to think that a pledge of confidentiality can be secured on a contractual basis. In most situations involving data extraction, the individual is in no position to demand a promise to this effect. Of course, the courts may change their attitude when the potentialities of the computer become apparent. But to wait for the courts to create common-law obligations and impose them on information extractors, processors, transmitters, and users for the benefit of data subjects will require the patience of Job and may prove to be no more fruitful than agitating for the expansion of the common-law privacy action. Time is a luxury personal privacy cannot afford and the glacial movement of legal doctrine is inappropriate for the problem at hand.

ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 220 (1971).

[17] One insightful commentator has recognized that the "advent of widespread use of computer technology . . . has altered the way in which individuals view the world . . . . Today, lawyers and business professionals must be cognizant of communications law, criminal law, privacy law, and many other subjects that may not have been relevant to their situation only a decade ago." RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY: RIGHTS, LICENSES, LIABILITIES, III-1 (2d ed. 1992).

[18] The so-called exclusionary rule has had its critics. Almost two decades after the exclusionary rule had been adopted in *Mapp v. Ohio*, 367 U.S. 643 (1961), President

*United States v. Kramer*, a federal appellate court was asked to decide whether a telephone used in committing the crime at issue was a "computer."[19]

## I. THE *KRAMER* DECISION

In what can be fairly described as an opinion that centered on only one definition that will no doubt affect many, a court was asked to categorize a cellular telephone as a computer, as described in certain federal criminal statutes.[20] The troubling facts involved Neil Kramer's conviction of a crime against a fifteen-year-old female from Missouri who inadvertently sent a text message to Kramer's phone, beginning a seven-month period of "text messaging and telephonic communication."[21] Kramer was made aware of the victim's age.[22] In November of 2008, Kramer met the victim at a Missouri convenience store after driving from his home in Louisiana.[23] "The pair drove to the Comfort Inn in Willow Springs, Missouri, where he plied the victim with illegal narcotics and then engaged in sexual intercourse with her."[24] The day after their first sexual encounter, the victim was transported to Kramer's trailer located in Violet, Louisiana. On Friday 14, 2008, the victim was able to text her mother, reporting her location from a Louisiana bar.[25] Members of the St. Bernard

---

Ronald Reagan established a commission which recommended it be abolished. In its report, the task force explained:

> Legislation should be proposed and enacted to abolish the exclusionary rule as it is applies to Fourth Amendment issues. . . . Anyone evaluating the exclusionary rule must constantly keep this basic premise in mind. The framers of the Constitution did not create the exclusionary rule for violations of the Fourth Amendment. They could have done so. . . . The exclusionary rule is instead a judicially created rule of procedure that fails to serve the goals it seeks, and fails at a tremendous cost.

PRESIDENT'S TASK FORCE ON VICTIMS OF CRIME FINAL REPORT 24-25 (1982), *available at* http://www.ojp.gov/ovc/publications/presdntstskforcrprt/welcome.html.

[19] 631 F.3d 900 (8th Cir. 2011).

[20] *See* Brief for the United States at 1, United States v. Kramer, 631 F.3d 900 (8th Cir. 2011) (No. 10-1983).

[21] *Id.* at 4.

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.* at 5.

Parish Sherriff's Department responded to the bar.[26] Kramer was subsequently arrested in the parking lot of the bar, and the victim was reunited with her family.[27]

On December 21, 2009, Kramer pleaded guilty to the charge of transportation of a minor with the intent to engage in criminal sexual activity, in violation of 18 U.S.C. § 2423(a).[28] Although Kramer admitted to the unlawful behavior, his real dispute in the courts focused on the consequences of his action: the length of his incarceration. Under the federal statutes at issue, if it was found that Kramer used a computer to commit his crimes, his sentence could be substantially increased. The definition of "computer" became a controversial focal point as the case moved through the court system.

At his sentencing hearing, Kramer argued that the evidence was inadequate to establish that his cell phone was, in fact, a computer.[29] Among Kramer's arguments was that his phone did not access the Internet.[30] The government countered by arguing that Kramer's cellular phone could act "as a calculator, [while also] storing music, digital photographs, and video . . . ."[31] The district court judge agreed with the prosecutor's position, concluding that Kramer's cellular phone was, in every important respect, indistinguishable from a traditional computer.[32] That finding allowed a "two-level" enhancement of Kramer's punishment under federal sentencing law.[33] Kramer appealed his conviction, which was affirmed on February 8, 2011, in an opinion by Judge Wollman.[34]

In reaching his decision, the judge quoted one of the modern innovators of computers at the outset of his opinion. The judge quoted Steve Wozniak, co-founder of Apple Computer, recently commenting that "[e]verything has a computer in it nowadays."[35]

---

[26] *Id.*
[27] *Id.*
[28] *Id.* at 3.
[29] *Id.* at 6.
[30] *Id.* at 12.
[31] *Id.* at 10.
[32] *Id.* at 6.
[33] *Id.* at 7.
[34] United States v. Kramer, 631 F.3d 900, 900-01 (8th Cir. 2011).
[35] *Id.* at 901.

He posed the question at issue in the appeal of whether an ordinary cellular phone—used only to place calls and send text messages—constituted a computer.[36] He observed that the district court, relying on the definition of "computer" found in 18 U.S.C. § 1030(e)(1), enhanced Neil Kramer's sentence for transporting a minor in interstate commerce with the intent to engage in criminal sexual activity with her, a violation of 18 U.S.C. § 2423(a).[37]

Judge Wollman noted that at trial, defendant Kramer "acknowledged that he used his cellular telephone—a Motorola Motorazr V3—to make voice calls and send text messages to the victim for a six-month period leading up to the offense."[38] At the earlier proceedings, the district court concluded that Kramer's cellular phone was a "computer" pursuant to 18 U.S.C. § 1030(e)(1).[39] The district court then "applied a two-level enhancement for its use to facilitate the offense, *see* U.S. Sentencing Guidelines Manual § 2G1.3(b)(3) (2009), and sentenced Kramer to 168 months' imprisonment."[40] Although the sentence given by the judge was "within both the original and enhanced guidelines ranges, the district court acknowledged that without the enhancement it would have sentenced Kramer to 140 months' imprisonment."[41] The judge's statement about enhancement made it clear that he was relying on the fact that the phone was a computer for purposes of increasing Kramer's punishment.

Noting an objection to the judge's ruling, Kramer argued "that application of the enhancement was procedural error because a cellular telephone, when used only to make voice calls and send text messages, cannot be a 'computer' as defined in 18 U.S.C. § 1030(e)(1)."[42] Kramer further complained that "even if a phone could be a computer, the government's evidence was insufficient to show that his phone met that definition."[43] The U.S. Sentencing Guidelines Manual § 2G1.3(b)(3) provides a two-level

---

[36] *Id.* at 902.
[37] *Id.* at 901.
[38] *Id.* at 901-02.
[39] *See* United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).
[40] *Id.* at 902.
[41] *Id.*
[42] *Id.*
[43] *Id.*

enhanced punishment for "the use of a computer . . . to . . . persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct . . . ."[44]

The broad definition of "computer" in criminal statute 18 U.S.C. § 1030(e)(1),[45] provides that any "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 . . . ."[46] might satisfy the statutory requirements to qualify as a computer. It is clear, however, that "an automated typewriter or typesetter, a portable hand held calculator, or other similar device" would not be included in the definition of a computer.[47]

Kramer believed that "the district court incorrectly interpreted the term 'computer' to include a 'basic cell phone'" that he used only to call and send text messages to the victim.[48] The circuit court rejected Kramer's view that the sentencing "enhancement should apply only when a device is used to access the Internet."[49] Relying on the broad language of 18 U.S.C. § 1030(e)(1), the court held that "an electronic . . . or other high speed data processing device performing logical, arithmetic, or storage functions," is a computer.[50] The court noted that "[t]his definition captures any device that makes use of a [sic] electronic data processor, examples of which are legion."[51]

Kramer argued before the trial court that the word "electronic" modifies "high speed data processing device"[52] and therefore the device must be both "electronic" and "high speed."[53] The government countered that argument by asserting that "electronic, magnetic, optical, [and] electrochemical"[54] data

---

[44] *Id.*

[45] *See* U.S. Sentencing Guidelines Manual § 2G1.3(b)(3) cmt. at 205 n.1 (2009) ("'Computer' has the meaning given that term in 18 U.S.C. § 1030(e)(1).").

[46] *Id.*

[47] *Id.*

[48] United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

[54] *Id.*

processing devices are, by their nature, "high speed."[55] Further, they argued that the language, "other high speed," was included by Congress "to expand the statute to cover additional types of high-speed devices that were not, or could not be, enumerated."[56] After considering both arguments, the circuit court decided not to resolve the disputed reading of the statute. It reasoned that "even if Kramer's reading of the statute is correct, a modern cellular phone can be a 'high speed' electronic device" and thus qualify a defendant for an enhanced penalty.[57] The circuit court further explained: "Indeed, modern cellular phones process data at comparable or faster rates than the desktop computers that existed when § 1030(e)(1) was enacted."[58]

The court noted in dicta that a high speed electronic storage device could potentially 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."[59]

It further explained that "each time an electronic processor performs any task—from powering on, to receiving keypad input, to displaying information—it performs logical, arithmetic, or storage functions. These functions are the essence of its operation."[60]

The circuit court also concluded that there was "nothing in the statutory definition that purports to exclude devices because they lack a connection to the Internet."[61] Although the court acknowledged that the term computer "does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device,"[62] it did not think Congress

---

[55] *Id.*

[56] *Id.*

[57] *Id.* at 903 n.3.

[58] *Id.*

[59] *Id.* at 903 (quoting Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010)) (internal quotation marks omitted).

[60] United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).

[61] *Id.*

[62] *Id.*

intended to exclude all non-Internet-enabled devices from the definition of "computer."[63]

Although the circuit court acknowledged that a "basic" cellular phone might not easily fit within the colloquial definition of "computer,"[64] the court asserted it was bound "not by the common understanding of that word, but by the specific—if broad—definition set forth in § 1030(e)(1)."[65] The court surprisingly acknowledged that "it may be that neither the Sentencing Commission nor Congress anticipated that a cellular phone would be included in that definition."[66]

At the district court hearing, "[t]he government did not, however, offer any expert testimony regarding the phone's capabilities."[67] The circuit court noted that "the materials presented to the district court were sufficient to show by a preponderance of the evidence that Kramer's phone was an 'electronic . . . or other high speed data processing device' that 'perform[ed] logical, arithmetic, or storage functions' when it was used by Kramer to call and text message the victim."[68]

From the phone's user's manual presented to the trial court by the prosecution, "the phone is powered by a '680 mAh Li-ion' battery, has '5MB' of memory, is capable of running software, makes use of a 'Graphic Accelerator' to run its color display screens, has a 'User-customizable' main menu, and comes with 'Preloaded' text messages."[69]

The user's manual "warns that the phone may include copyrighted Motorola and third-party software stored in semiconductor memories or other media."[70] Thus, these features "are sufficient to show that the phone makes use of an electronic data processor . . . [and] performs arithmetic, logical, and storage functions when the phone is used to place a call. The user's manual notes that the phone 'keeps lists of incoming and outgoing

---

[63] *Id.*

[64] *Id.*

[65] United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).

[66] *Id.*

[67] *Id.* at 904.

[68] *Id.*

[69] *Id.* (internal citations omitted).

[70] United States v. Kramer, 631 F.3d 900, 904 (8th Cir. 2011) (internal quotations omitted).

calls, even for calls that did not connect.'"[71] Furthermore, cell phones tracked "the elapsed time from the moment [the user] connect[s] to [the] service provider's network to the moment [the user] end[s] the call by pressing [the end key]."[72] The phone's counting function was a key element supporting the circuit court's finding that the phone met the requirements of the statute.[73] These capabilities all supported the district court's conclusion that the phone performed arithmetic, logical, and storage functions when Kramer used it to send text messages to the victim.[74]

## II. WHY IS THE *KRAMER* DECISION IMPORTANT FOR THE FUTURE?

A simple judicial decision defining a basic term in a statute should not raise an eyebrow given that courts perform such a function daily. The *Kramer* decision seems to fit the mold of an ordinary opinion at first glance. Upon closer examination, the case sends a subtle message of legislative responsibility for the language that it creates. The opinion curiously begins by citing one of the icons of the high technology age, one of Apple Computer's founders.[75] By starting the opinion with this acknowledgment of innovation in communications technology, one might suspect the movement of technology would play a prominent role in the opinion. Yet this was not the case. The judge paid only minor lip service to the technological ramifications of defining nearly every modern cell phone as a computer for the purpose of federal sentencing enhancement.

Using a dictionary definition approach[76] to decide the case, the court mentioned little of the long-term importance of its opinion on future criminal investigations or other matters involving emerging technology. If the clear outcome of *Kramer* dictates the use of simple statutory construction in defining

---

[71] *Id.*

[72] *Id.*

[73] *Id.* at 905.

[74] *Id.*

[75] United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011).

[76] *See* THE NEW OXFORD AMERICAN DICTIONARY 277 (2d ed. 2005) (defining "central processing unit" as "the part of a computer in which operations are controlled and executed").

"computer," then perhaps the question is settled.[77] Privacy advocates may feel there is no need for alarm. Indeed, law enforcement is no doubt content with the outcome that a defendant like Neil Kramer can be punished more severely because he used a "computer" to commit his crime. The police, after all, can be expected to use the full arsenal of weapons at their disposal to detect and prove criminal activity.[78] After all, Kramer committed what many feel is the most serious crime of all—a sexual offense against a minor.[79] Surely Congress could not be faulted for trying to achieve the goal of severely punishing such offenders. Assuming Congress intended such a broad definition of a computer as the court in *Kramer* suggests, what does *Kramer*'s holding mean for other courts facing similar questions involving emerging technologies?

Think about the type of evolving technologies that routinely seize and store all kinds of information that some may consider private. Every time a vehicle goes through a toll booth the tag is recorded and linked to whatever sensitive information is attached to that registered vehicle's owner.[80] Similarly, speed and red light

---

[77] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010) ("Just think of the common household items that include microchips and electronic storage devices, and thus will satisfy the statutory definition of 'computer.'").

[78] Thomas K. Clancy, noted this flexibility in law enforcement:

> Crime has changed, as have the means of law enforcement, and it would therefore be naive to assume that those actions a constable could take in an English or American village three centuries ago should necessarily govern what we, as a society, now regard as proper. Thus, the Court has sometimes asserted that the Amendment's "prohibition against 'unreasonable searches and seizures' must be interpreted 'in light of contemporary norms and conditions.'"

Thomas K. Clancy, *What Constitutes an "Arrest" Within the Meaning of the Fourth Amendment?*, 48 VILL. L. REV. 129, 184 (2003) (footnote omitted) (quoting Steagald v. United States, 451 U.S. 204, 217 n.10 (1981)) (internal quotation marks omitted).

[79] Law enforcement obviously needs data in order to investigate and prosecute crime. High technology has proven particularly useful in the prosecution of offenders engaged in child pornography. *See* Jason Krause, *Can Anyone Stop Internet Porn?: Courts Have Shot Down Laws Protecting Kids from Obscenity Online. Is Cyberspace Suited for a Virtual Privacy Wrapper?*, 88 A.B.A. J., Sept. 2002, at 56.

[80] Public use of intrusive video technology is growing. *See* M.J. Zuckerman, *Chances Are, Somebody's Watching You*, USA TODAY, Nov. 30, 2000, at 01.A (describing a forty million dollar surveillance center using 110 remote control cameras in the suburbs of Washington).

photo cameras record images[81] of a driver and his or her passengers while noting the time of travel.[82] Gasoline purchase records document how much fuel is in a vehicle and the location of purchase with startling accuracy.

When a customer shops for groceries, the store records the customer's purchases to identify preferences. These records of tastes and prior choices are recorded to allow the merchant to offer a coupon to purchase your favorite tissue paper days before it runs out. Cellular phones are capable of locating individuals almost anywhere in the world with startling accuracy. All of these intrusions are given little thought because of the conveniences the technology brings to our lives. Instant coupons, weekly special values, discounts for future purchases, and other inducements make us surrender our e-mail addresses to take advantage of these benefits. In short, citizens love the ease and comfort these technologies afford.

Law enforcement has benefited greatly from the accuracy of record keeping that the computer era has provided. Little thought is given to where this information "lives" or is stored when it is waiting to be reviewed or retrieved.[83] It is usually unclear who

---

[81] New forms of surveillance technology that actually record facial images and compare features to other persons located in computer databases have been increasingly used by law enforcement. *See* Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 303-08 (1999) (describing digital and biometrics technology).

[82] Consider, as an example of intrusion, the use of red light cameras, which has emerged over the last decade. Currently, the surveillance method is so common that we are no longer surprised by the mailed notices, capturing our vehicle and often a passenger, the time of violation, and our exact location at a camera-equipped intersection. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). One federal court had this comment about the law:

> The passage of the Patriot Act altered and to some degree muddied the landscape. In October 2001, Congress amended FISA [Foreign Surveillance Intelligence Act] to change "the purpose" language . . . . It also added a provision allowing "Federal officers who conduct electronic surveillance to acquire foreign intelligence information" to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents.

*In re* Sealed Case Nos. 02-001, 02-002, 310 F.3d 717, 728-29 (FISA Ct. Rev. 2002).

[83] If there is any doubt that the government continues to construe *Smith v. Maryland*, 442 U.S. 735 (1979), with any less than the broadest possible scope, the

has permission to review this information. These concerns have raised little alarm so long as a better "smart phone" is on the way soon.[84]

One might suggest that in many of the concerns I raise the user of the technology knowingly and willingly exposes their information to third parties—in the cases of seized photographic images, they may not be considered private at all.[85] Furthermore, since much of the information that I have complained about is not seized by government officials, it is not private at all or even subject to Fourth Amendment review. Even when the Fourth Amendment is implicated, courts sometimes struggle with where the line of protection should be drawn when new technologies are

---

testimony of Deputy Associate Attorney General Kevin DiGregory during a congressional hearing on government surveillance issues is instructive. DiGregory said:

> [T]he Supreme Court held, in Maryland versus Smith [sic], I believe, in 1979, that there was no reasonable expectation of privacy in numbers dialed by a telephone, because essentially, when someone turns over information to a third party, like the telephone company, they should not have either a subjective or an objective reasonable expectation of privacy in that information.

*Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000) (emphasis added) (statement of Kevin V. DiGregory, Deputy Assoc. Att'y Gen., U.S. Dep't of Justice).

[84] All eyes have been trained on News Corp. in recent weeks, following allegations that the now-defunct *News of the World* hacked the phones of more than 4000 politicians, crime victims, and celebrities:

> [T]he art of getting people to inadvertently divulge information through seemingly innocuous questions—is one way, and it's as simple as going on a website and tricking a system or individual. For example, Christopher Soghoian, a fellow at the Center for Applied Cypersecurity [sic] Research, in a quick email shared a website called phonegangster.com. The website can send visitors directly to a voicemail account, where they can insert a pass code by spoofing a phone number.

Lyneka Litle, *Murdoch Scandal Fallout: Consumers Make Cell Phone Hacking Easy*, ABC NEWS (July 22, 2011), http://abcnews.go.com/Business/murdoch-scandal-fallout-consumers-make-cell-phone-hacking/story?id=14128470&singlePage=true.

[85] The storing of visual images, in general, raises many concerns in society. "Video-surveillance cameras quietly scan many workplaces. Neighborhood retailers now stock hardware that used to be the stuff of spy novels." Richard Lacayo, Tom Curry, Thomas McCarrol & Dennis Wyss, *Assaulting Our Privacy: Nowhere to Hide*, TIME, Nov. 11, 1991, at 34.

involved.[86] Thus, we may have surrendered our personal information without much thought as to who might retrieve it or if we can limit its use. We have simply allowed it to be sent to the winds, incapable of ever controlling it again.[87] With the exception of some medical[88] and financial data,[89] very little statutory protection is provided for much of the information routinely communicated over our "computer phones." Has this truly been a willing choice, or have we simply been enchanted by the science of communication?[90] Perhaps it does not matter anymore. The average citizen has lost so much control over their personal information that it may be impossible to reverse the trend.[91]

---

[86] Tracey Maclin, Katz*,* Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51-52 (2002) ("Advances in science and technology recurrently exert pressure on the scope and meaning of the Fourth Amendment, but the privacy and security protected by the Fourth Amendment should not depend on innovations and technology. . . . During the Framers' era, the home was the focal point of privacy and personal security." (footnote omitted)). "When the American Republic was founded, the framers established a libertarian equilibrium among the competing values of privacy, disclosure and surveillance." ALAN F. WESTIN, PRIVACY AND FREEDOM 67 (1967).

[87] One scholar has gone so far as to suggest that "[i]n this era of rapid technological change, the freedom to be unnoticed in public, and its associated benefits, will disappear unless a right to public anonymity is recognized and enforced." Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 217, 314-15 (2002) (arguing that the Fourth Amendment should be construed to recognize a right to public anonymity as a part of privacy expectations because "government surveillance of our innocent public activities that are not meant for public consumption is neither expected nor to be condoned").

[88] Tracey Maclin, *Let Sleeping Dogs Lie: Why the Supreme Court Should Leave Fourth Amendment History Unabridged*, 82 B.U. L. REV. 895, 933-34 (2002). The Supreme Court rejected a challenge to a New York central computer databank containing the names and addresses of all persons obtaining drugs by prescription.

[89] United States v. Miller, 425 U.S. 435, 442-43 (1976) (citing United States v. White, 401 U.S. 745, 751-52 (1971)) (finding no reasonable expectation of privacy in financial information contained at the defendant's bank because a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the [g]overnment"); FRANK J. DONNER, THE AGE OF SURVEILLANCE 7 (1980).

[90] *See* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 425 n.386 (2002) ("As society has evolved and our lives have become more mobile, as we spend more and more of our waking hours away from home, there may be even more reason to prize our right to preserve secrecy outside dwellings and to be concerned with novel perils generated by scientific and technological progress.").

[91] "Repeated invasions by credit bureaus, employers, and the like can lead persons to discount most expectations as unreasonable; individual fears of a loss of privacy then become self-fulfilling prophecies. In particular, the government can through its actions

Perhaps the benefits of technology are so great we simply do not care about how our privacy has been diminished.[92] Perhaps the *Kramer* court's casual approach to controlling emerging technology reflects our casual attitude toward the protection of privacy.[93]

## CONCLUSION

Maybe there is no Big Brother[94] to worry about after all, only Little Brother! If we like that law enforcement is having an easier time prosecuting crime because of the computer, there is no need to be alarmed. If we want our local grocer to remind us we are running out of coffee, we are happy for them to evaluate our kitchen closet.[95] If we want our computer to remember the web site we visited a week ago to get a recipe, perhaps we do not mind if our internet service provider sells our information to a cooking

---

redefine popular expectations so as to undermine constitutional rights." Comment, *Legitimate Expectations of Privacy Against Unreasonable Searches and the "Automatic Standing Rule,"* 94 HARV. L. REV. 196, 203 (1980).

[92] The value of personal privacy has been a concept that many thinkers have pondered for well over a century. One particularly longstanding comment of privacy reminds us that "[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. . . . [T]he right to be let alone . . . has grown to comprise every form of possession—intangible, as well as tangible." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1891).

[93] The challenge for the *Kramer* court was to take seriously the very real threat posed to societal privacy by what appears to many to be a routine case. Such decisions also pose a danger of courts being too casual with their role as protector of individual liberty. One insightful commentator has noted that "technological advances pose the challenges that always beset the constitutional enterprise—those involved with trying to create fixed rules, or at least a workable rule of law, for a changing world." Susan Bandes, *Power, Privacy and Thermal Imaging*, 86 MINN. L. REV. 1379, 1383 (2002).

[94] M. ETHAN KATSH, LAW IN A DIGITAL WORLD 227-28 (1995) ("In Orwell's society, there was no right of privacy or expectation of privacy. In our society, privacy is highly valued and some legal rights of privacy do exist. Yet privacy, in the sense of being able to control information about oneself, is also an eroding condition." (footnote omitted)).

[95] Whalen v. Roe, 429 U.S. 589, 605 (1977) ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.").

school.[96] In an age when fear of terrorism dominates both the need and the use of intrusive technology,[97] we are likely to discount the very protections envisioned by our Founding Fathers in the Bill of Rights. Again, we are often reminded that the desire to be secure should always dominate our need to choose more privacy when intrusion becomes both quick and easy.

Perhaps George Orwell was correct about the final outcome of all this technology when he said, "Forty years it had taken him to learn . . . . O cruel, needless misunderstanding! . . . But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother."[98] Perhaps we

---

[96] An important aspect of electronic searches is their potential scope. They are not merely limited to information or historical facts, but also permit access to discovering future events. As one commentator explained:

> The conventional search is limited to a designated thing in being—one of a finite number of things to be found in the place where the search is to be conducted, and ordinarily discoverable in a single brief visit. On the other hand, electronic surveillance is a quest for something which may happen in the future. Its effectiveness normally depends upon a protracted period of lying-in-wait. For however long that may be, the lives and thoughts of many people—not merely the immediate target but all who chance to wander into the web—are exposed to an unknown and undiscriminating intruder. Such a search has no channel and is certain to be far more pervasive and intrusive than a properly conducted search for a specific, tangible object at a defined location.

Ralph S. Spritzer, *Electronic Surveillance by Leave of the Magistrate: The Case in Opposition*, 118 U. PA. L. REV. 169, 189 (1969).

[97] David Hardin, Note, *The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 345 (2003) ("Although the conflicting interests involved are compelling, the paramount function of national security is to vigilantly protect the ideals embodied by the very same Amendment that the standard violates. Those ideals cannot be whittled away in today's desire to defend the very same values that provide for our security.").

[98] ORWELL, *supra* note 2. In a recent Supreme Court oral argument regarding whether it was constitutional for the government to track anyone it choose by attaching a Global Positioning Satellite device on their vehicle (GPS), the following exchange occurred between the government attorney and Chief Justice John Roberts, reflecting the potential consequences of the government's willingness to use technology in law enforcement:

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The justices of this Court?

should think about what we are giving up and not be so quick to fall in love.[99]

---

> CHIEF JUSTICE ROBERTS: Yes. (Laughter.)
>
> MR. DREEBEN: Under our theory and under this Court's cases, the justices of this Court when driving on public roadways have no greater expectation
>
> CHIEF JUSTICE ROBERTS: So your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?
>
> MR. DREEBEN: Well, equally, Mr. Chief Justice, if the FBI wanted to it could put its team of surveillance agents around the clock on any individual and follow that individual's movements as they went around on the public streets and they would thereby gather . . . .

Transcript of Oral Argument at 9-10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10–1259).

[99] It has been argued that a "good society must have its hiding places—its protected crannies for the soul. Under the pitiless eye of safety the soul will wither." Charles A. Reich, *Police Questioning of Law Abiding Citizens*, 75 YALE L.J. 1161, 1172 (1965).