NACDL
FOURTH
AMENDMENT
CENTER

July 11, 2022

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

INTRODUCTION

The National Association of Criminal Defense Lawyers (NACDL) is the preeminent organization in the United States advancing the goal of the criminal defense bar to ensure justice and due process for persons charged with a crime or wrongdoing. NACDL serves as a leader in identifying and reforming flaws and inequities in the criminal legal system and ensuring that our members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

NACDL insists that any guidance regarding forensic searches of digital devices should, at the very least, acknowledge the legal and constitutional concerns that such searches present. As our lives migrate increasingly to the digital realm, computers and cellphones have become maps of our political and religious affiliations, our sexual preferences, our networks of social and professional relationships, and more. While the National Institute of Standards and Technology (NIST) is not responsible for resolving the complex legal and constitutional questions that digital forensic investigations raise, it would be irresponsible for NIST's technical guidance on this subject to ignore the privacy interests—and the attendant legal and constitutional concerns—that are implicated by sweeping intrusions into a person's digital life.

The purpose of this comment is not to challenge the technical guidance presented in NIST's report on digital forensics, but rather to urge NIST to include a disclaimer regarding the contested legality and constitutionality of the techniques outlined in its report. As technology evolves, so does Fourth Amendment jurisprudence on digital device searches. It is therefore imperative that any guidance on such a sensitive issue—particularly from a government agency—acknowledge the legal limits of its recommendations.

COMMENT

Computers, cellphones, and other digital devices are repositories of deeply personal information. In the pre-digital age, people conducted their financial business at the bank, their medical affairs at the doctor's office, their political activism in community centers, and their romantic dalliances on landlines and via letters. Now, all that information and more is consolidated on their digital devices. A computer or cellphone is less like a file cabinet than it is like the inside of a person's brain.[1] As the Supreme Court noted in *California v. Riley*—and again in *United States v. Carpenter*—digital devices contain "the privacies of life."[2] Because the data and metadata stored on—and accessible from—these devices are so revealing, courts are contending in real time with rapid technological evolution and the migration of quotidian private activities to the digital sphere.[3]

The Fourth Amendment of the United States Constitution protects against "unreasonable searches and seizures" and requires that all warrant applications be based upon probable cause and include a "particular[] descri[ption] [of] the place to be searched."[4] These requirements were

---

[1] *Contra* Nat'l Inst. of Standards and Tech., *Digital Investigation Techniques: A NIST Foundation Review* 7 (May 2022), https://perma.cc/MC2W-QFGY (analogizing categories of "real-world" evidence to "digital-world" evidence).
[2] *Riley*, 573 U.S. 373, 403 (2014) (citation omitted); *Carpenter*, 138 S. Ct. 2206, 2210 (2018).
[3] *See Public Safety, Privacy, and Particularity: A New Approach to Search Warrants for Digital Evidence*, Bloomberg Law (June 17, 2014), https://perma.cc/5WZZ-TCBS (describing circuit split on protocols for computer searches).
[4] U.S. Const., amend. IV.

codified in the Constitution largely in opposition to the general warrants and writs of assistance that "allowed British officers to rummage through [papers and effects] in an unrestrained search for evidence of criminal activity."[5] The probable cause requirement demands that there be "a fair probability that contraband or evidence of a crime will be found in a particular place"[6] and the particularity requirement defines a valid warrant as one that limits searches and seizures to evidence that is related to a specific crime.[7] Courts have spent the past half-century interpreting these requirements largely in the analog world; now, they are in the process of translating that jurisprudence to the wild west of the digital realm.

The debate over what the probable cause and particularity requirements mean when it comes to digital device searches is focused largely on the sort of investigative techniques that NIST describes in its draft report on digital forensics.[8] Digital forensics investigations frequently involve wholesale search and seizure of digital information. Courts are increasingly concerned with the constitutionality of such limitless searches and seizures. NIST's report recommends far-reaching digital forensics techniques, including copying entire hard drives,[9] recovering deleted data,[10] and more. While it may be that NIST's report recommends the most efficient and comprehensive methods for conducting forensic investigations of digital devices, it remains an open question whether those methods are constitutional. In fact, many courts have already held that indiscriminate searches and seizures of digital device data are unconstitutional.[11]

---

[5] *Riley*, 573 U.S. at 403.
[6] *Illinois v. Gates*, 462 U.S. 213, 238 (1983).
[7] *See Andresen v. Maryland*, 427 U.S. 463, 481–83 (1976).
[8] *See supra*, n.1.
[9] *See id.* at 34.
[10] *See id.* at 36
[11] *See, e.g., United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement."); *United States v. Morales*, 77 M.J. 567, 573 (A. Ct. Crim. App. 2017) (holding that there was probable cause to search text messages on defendant's phone, but not photographs); *United States v. Winn*, 79 F. Supp. 3d 904, 922 (S.D. Ill. 2015) (holding that warrant containing "unabridged template that authorized the police to seize the entirety of the phone and rummage through every conceivable bit of data" was unconstitutional and that complaint established probable cause only for "a very small and specific subset of data on [the] cell phone"); *In re*

As courts continue to identify and define the constitutional boundaries of digital device searches, the technical guidance governing digital forensics will likely have to adapt to the evolving jurisprudential reality. Because the legal standards are in flux—and indeed, are hotly contested by parties interested in the privacy rights of criminal defendants—it is incumbent upon NIST to state in unequivocal terms that its recommendations are purely technical and do not necessarily conform to legal and constitutional requirements.

CONCLUSION

Digital devices contain vast quantities of deeply personal, far-ranging, and revealing information. Consequently, digital searches are qualitatively different from their analog equivalents. The Fourth Amendment's probable cause and particularity requirements raise special concerns for searches and seizures of digital information. In providing technical guidance on digital forensics, NIST should be careful not to misrepresent the legality and constitutionality of the investigative techniques that it describes. At the very least, NACDL recommends that NIST insert a disclaimer in its report acknowledging the ongoing legal debate over the permissible scope of digital device searches. NIST's report should further state, in explicit terms, that its guidance is purely technical in nature and does not reflect contemporary jurisprudence on the constitutional limits of digital device searches.

Nextel Cellular Tel., No. 14-MJ-8005-DJW, 2014 WL 2898262, at *13 (D. Kan. June 26, 2014) ("[J]ust as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe drug trafficking communication may be found in [the] phone's [] mail application will not support the search of the phone's Angry Birds application.") (citation and quotation marks omitted).