FOREWORD

THE SEARCH AND SEIZURE OF COMPUTERS AND ELECTRONIC EVIDENCE

Thomas K. Clancy[*]

The National Center for Justice and the Rule of Law,[1] a program of the University of Mississippi School of Law, focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. In furtherance of its mission, the Center has established the *Fourth Amendment Initiative*. Perhaps no other Amendment has such broad applicability to everyday life as does the Fourth Amendment. The Fourth Amendment is also a very complicated area of jurisprudence and the legal landscape is constantly changing as a result of new technology and court decisions. The purpose of the Center's initiative is to promote awareness of Fourth Amendment principles through conferences, publications, and training of professionals in the criminal justice system. The Center takes no point of view as

---

[*] Director, National Center for Justice and the Rule of Law, and Visiting Professor, University of Mississippi School of Law.

[1] The National Center for Justice and the Rule of Law is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the U.S. Department of Justice, grant No. 2000-DD-VX-0032. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles stemming from this symposium are those of the author and do not represent the official position of the United States Department of Justice. For more information about the Center, please visit www.ncjrl.org.

to the direction that Fourth Amendment analysis should take but seeks to facilitate awareness of the issues and encourage discussion of search and seizure principles.

A central pillar of the Fourth Amendment Initiative is annual symposiums on important search and seizure topics. On February 17, 2005, the Center held its fourth annual symposium, *The Search and Seizure of Computers and Electronic Evidence*. The symposium coincided with the third day of a conference entitled *Advanced Training on Search and Seizure of Computers and Obtaining Electronic Evidence*, sponsored by the Center in cooperation with the National Association of Attorneys General, which was attended by approximately 64 prosecutors and others, from Attorneys General offices from 34 states, American commonwealths, and territories; for the symposium, they were joined by 55 lawyers, law students, and law professors, while another 219 persons observed the symposium via the Internet.

The Center believes that the conference and symposium–and the insightful articles published in this special edition of the *Mississippi Law Journal* that stemmed from the presentations at those events–significantly further the Center's mission and, more importantly, make significant contributions to the understanding of Fourth Amendment principles. The Center, and I personally, wish to thank the leading legal scholars who participated.

Susan Brenner, Professor at the University of Dayton School of Law, in her article, *The Fourth Amendment in an Era of Ubiquitous Technology*, poses the question whether the guarantee of privacy contained in the Fourth Amendment is adaptable to a world where technology is "increasingly pervasive–a world of ubiquitous technology." In answering the question, Brenner examines how the approach to privacy, which began as a "bricks and mortar" concept, evolved in the 20th Century to accommodate technological change. Brenner observes that the physical and informational barriers that once served to differentiate our public and private lives are rapidly

being eroded by technology. Thus, Brenner maintains, a spatial conception of the guarantee offered by privacy is no longer effective. Brenner offers insights on how to adapt the concept of privacy to accommodate the challenges of the 21st Century, that is, to a society where physical barriers have little, if any, meaning. An essential feature of information technology is the ability of others to "harvest" that information and Brenner discusses impediments to protecting such information, including the concepts of voluntary exposure and assumption of risk; she argues that the assumption of risk "calculus is an unreasonable methodology for a non-spatial world." Brenner, after observing that society acknowledges privacy protections for certain types of shared privacy, proposes expanding that concept to include information conveyed to "servant" entities who provide us with various types of support.

Orin Kerr, an Associate Professor at The George Washington School of Law, in his article *Search Warrants in an Era of Digital Evidence*, contends that the legal rules regulating the search warrant process must be revised in light of the demands of digital evidence collection. He asserts that existing rules are premised on the police obtaining a warrant to enter the place to be searched and then retrieving the property named in the warrant. Computer technologies, Kerr believes, tend to bifurcate the process into two steps: the police must first execute a physical search to seize the computer hardware and then later execute a second electronic warrant to obtain the data from the seized computer storage device. He asserts that the law has failed to account for that two-stage process and, hence, regulate the warrant process effectively. Kerr offers a series of proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure to update the warrant process for the era of digital evidence.

Christopher Slobogin, a Professor at the University of Florida Fredric G. Levin College of Law, in *Transaction Surveillance by the Government*, observes that many important aspects of our lives are inscribed in written and digitized records, housed in private businesses, government agencies, and other institutions. The records include all sorts of information

about us: reports on our medical status and financial condition; data about our purchases, rentals, real estate holdings, licenses, and memberships; logs listing the destination of our emails and our Internet wanderings; and countless other bits of individual descriptors, ranging from salary levels to college grades to driver's license numbers. Slobogin notes that there is often an understanding that the information will be used or viewed by a limited number of people for circumscribed purposes, that is, we consider the contents of many of the records private. His article explores what he calls "transaction surveillance" by the government, which involves accessing already-existing records, either physically or through computer databanks, and accessing the identifying signals of a transaction (such as the address of an email recipient). Slobogin observes that transaction surveillance is subject to far less regulation than either physical surveillance of activities inside the home or communications surveillance. He argues that transaction surveillance should be subject to much more legal monitoring than it is. He proposes recognizing that different sorts of records merit different levels of protection, significantly increasing the degree of protection to the probable cause level for personal records held by private and public entities and to the reasonable suspicion level for records readily available to the public. Although Slobogin examines several alternative approaches to affording protections to records, including legislative action, he concludes that only the Fourth Amendment, properly construed, has the ability to provide adequate protection.

In *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, I offer a "primer" that outlines the application of Fourth Amendment principles to the search and seizure of computers and the digital information that is stored in them. The article, however, departs from the role of a primer in two important respects. First, in discussing the nature of computer and digital evidence searches and seizures, it rejects the view that unique Fourth Amend-

ment rules are needed to regulate them; instead, I believe that computers are containers and the data they contain are mere forms of documents. This is to say that the principles applicable to document searches have equal application to electronic data searches. Second, the article rejects expansion of the private search doctrine, used by some courts to permit government agents to open data files that had not been opened during a preceding private party search and still not be a search within the meaning of the Fourth Amendment. Underlying both of these points of view is the perspective that a computer is a container of containers of documents, that is, each individual file is a separate container–just like each manila file in a filing cabinet is a container–that requires a separate opening to determine what is inside. This is to say that the mere fact that an item to be searched or seized is electronic evidence does not fundamentally change the Fourth Amendment analytical structure that governs.

Marc Harrold, who is Counsel for National Programs at the Center and a Visiting Professor at the University of Mississippi School of Law, writes *Computer Searches of Probationers—Diminished Privacies, "Special Needs" &* "'Whilst' Quiet *Pedophiles"—Plugging the Fourth Amendment into the "Virtual Home Visit."* This is an important topic, given the large number of child sex offenders and child pornographers who use the Internet to facilitate their crimes. Harrold discusses the Fourth Amendment framework that regulates governmental programs that monitor the computer and Internet use of persons on probation. He surveys the various technological and other tools that are available to facilitate that monitoring. Harrold examines the Supreme Court and lower court decisions in the area and concludes that the "special needs" doctrine, developed by the Supreme Court to assess the reasonableness of regulatory and other searches, will most likely serve as the basis of assessing the reasonableness of the searches of probationers' computers.