ASPEN PUBLISHERS

PRIVACY, INFORMATION, AND TECHNOLOGY

Second Edition

Daniel J. Solove
Professor of Law
George Washington University Law School

Paul M. Schwartz
Professor of Law
U.C. Berkeley Law School

Wolters Kluwer
Law & Business

AUSTIN BOSTON CHICAGO NEW YORK THE NETHERLANDS

http://lawschool.aspenpublishers.com

To contact Customer Care, e-mail customer.care@aspenpublishers.com, call 1-800-234-1660, fax 1-800-901-9075, or mail correspondence to:

Aspen Publishers
Attn: Order Department
PO Box 990
Frederick, MD 21705

Printed in the United States of America.

1 2 3 4 5 6 7 8 9 0

ISBN 978-0-7355-7910-1

Library of Congress Cataloging-in-Publication Data

Solove, Daniel J., 1972-
Privacy, information, and technology / Daniel J. Solove, Paul M. Schwartz. — 2nd ed.
p. cm.
ISBN 978-0-7355-7910-1
1. Privacy, Right of — United States. 2. Data protection — Law and legislation — United States. I. Schwartz, Paul M., 1959- II. Title.

KF1262.S664 2008
342.7308'58 — dc22

2008044313

created a new sunset of December 31, 2009 for USA PATRIOT Act sections 205 and 215 (which concern "roving" FISA wiretaps and FISA orders for business records), and for FISA's "lone wolf" amendments. This law also expanded the list of predicate offenses for which law enforcement could obtain wiretap orders.

C. DIGITAL SEARCHES AND SEIZURES

1. SEARCHING THE CONTENTS OF COMPUTERS

The Scope of Warrants to Search Computers. In *United States v. Lacy,* 119 F.3d 742 (9th Cir. 1997), the defendant challenged a search warrant authorizing the seizure of his computer hard drive and disks. The defendant contended that the warrant was too general because it applied to his entire computer system. The court upheld the warrant because "this type of generic classification is acceptable when a more precise description is not possible." Several other courts have followed a similar approach as in *Lacy*, upholding generic warrants. In *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999), the court reasoned: "A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs." *See also United States v. Hay*, 231 F.3d 630 (9th Cir. 2000) (following *Lacy* and upholding a "generic" warrant application).[58]

However, there are limits to the scope of a search of a computer. In *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), an officer obtained a warrant to search a computer for records about illegal drug distribution. When the officer stumbled upon a pornographic file, he began to search for similar files. The court concluded that these actions amounted to an expansion of the scope of the search and would require the obtaining of a second warrant.

In *United States v. Campos*, 221 F.3d 1143 (10th Cir. 2000), the defendant e-mailed two images of child pornography to a person he talked to in a chat room. The person informed the FBI, and the FBI obtained a warrant to search the defendant's home and computer. The agents seized the defendant's computer, and a search revealed the two images of child pornography as well as six other images of child pornography. The defendant challenged the search as beyond the scope of the warrant because the agents "had grounds to search only for the two images that had been sent." However, the court rejected the defendant's contention, quoting from the FBI's explanation why it is not feasible to search only for particular computer files in one's home:

> . . . Computer storage devices . . . can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is

[58] For more about computer searches, see Raphael Winnick, *Searches and Seizures of Computers and Computer Data*, 88 Harv. J.L. & Tech. 75 (1994).

> included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site. . . .
>
> Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The wide variety of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. . . . Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code embedded into the system as "booby trap"), the controlled environment of a laboratory is essential to its complete analysis. . . .

Computer Searches and Seizures. Searches and seizures for digital information in computers present some unique conceptual puzzles for existing Fourth Amendment doctrine. Thomas Clancy contends:

> [C]omputers are containers. . . . They . . . contain electronic evidence, that is, a series of digitally stored 0s and 1s that, when combined with a computer program, yield such items as images, words, and spreadsheets. Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers.[59]

But is a computer a single container or is each computer file its own container? Orin Kerr argues:

> A single physical storage device can store the private files of thousands of different users. It would be quite odd if looking at one file on a server meant that the entire server had been searched, and that the police could then analyze everything on the server, perhaps belonging to thousands of different people, without any restriction.[60]

Is copying a computer file or other digital information a seizure under the Fourth Amendment? In *United States v. Gorshkov*, 2001 WL 1024026 (W.D. Wash. 2001), the FBI remotely copied the contents of the defendant's computer in Russia. The court held: "The agents' act of copying the data on the Russian computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant's or anyone else's possessory interest in the data." However, as Susan Brenner and Barbara Frederiksen contend:

> [T]he information contained in computer files clearly belongs to the owner of the files. The ownership of information is similar to the contents of a private conversation in which the information belongs to the parties to the conversation. Copying computer data is analogous to recording a conversation. . . . Therefore, copying computer files should be treated as a seizure.[61]

---

[59] Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193, 196 (2005).

[60] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 556 (2005).

[61] Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. & Tech. L. Rev. 39, 111-12 (2002).

Password-Protected Files. In *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001), Notra Trulock and Linda Conrad shared a computer but maintained separate files protected by passwords. They did not know each other's password and could not access each other's files. When FBI officials, without a warrant, asked to search and seize the computer, Conrad consented. The court held that the FBI could not search Trulock's files since Trulock had not consented:

> Consent to search in the absence of a warrant may, in some circumstances, be given by a person other than the target of the search. Two criteria must be met in order for third party consent to be effective. First, the third party must have authority to consent to the search. Second, the third party's consent must be voluntary. . . .
>
> We conclude that, based on the facts in the complaint, Conrad lacked authority to consent to the search of Trulock's files. Conrad and Trulock both used a computer located in Conrad's bedroom and each had joint access to the hard drive. Conrad and Trulock, however, protected their personal files with passwords; Conrad did not have access to Trulock's passwords. Although Conrad had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files.

UNITED STATES V. ANDRUS

483 F.3d 711 (10th Cir. 2007)

[Federal authorities believed that Ray Andrus was downloading child pornography to his home computer. Ray Andrus resided at his parents' house. Federal officials obtained the consent of Dr. Andrus (Andrus's father) to search the home. He also consented to their searching any computers in the home. The officials went into Ray Andrus's bedroom and a forensic expert examined the contents of the computer's hard drive with forensic software. The software enabled direct access to the computer, bypassing any password protection the user put on it. The officials discovered child pornography on the computer. Later on, the officials learned that Ray Andrus had protected his computer with a password and that his father did not know the password. Is the father's consent to search the computer valid since he did not know the password?]

MURPHY, J. . . . Subject to limited exceptions, the Fourth Amendment prohibits warrantless searches of an individual's home or possessions. Voluntary consent to a police search, given by the individual under investigation or by a third party with authority over the subject property, is a well-established exception to the warrant requirement. Valid third party consent can arise either through the third party's actual authority or the third party's apparent authority. A third party has actual authority to consent to a search "if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes." Even where actual authority is lacking, however, a third party has apparent authority to consent to a search when an officer reasonably, even if erroneously, believes the third party possesses authority to consent. *See Georgia v. Randolph,* 547 U.S. 103 (2006).

Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search. When the property to be searched is an object or container, the relevant inquiry must address the third party's relationship to the object. In *Randolph,* the Court explained, "The constant element in assessing Fourth Amendment reasonableness in consent cases . . . is the great significance given to widely shared social expectations." For example, the Court said, "[W]hen it comes to searching through bureau drawers, there will be instances in which even a person clearly belonging on the premises as an occupant may lack any perceived authority to consent." . . .

It may be unreasonable for law enforcement to believe a third party has authority to consent to the search of an object typically associated with a high expectation of privacy, especially when the officers know or should know the owner has indicated the intent to exclude the third party from using or exerting control over the object.

Courts considering the issue have attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence. Individuals' expectations of privacy in computers have been likened to their expectations of privacy in "a suitcase or briefcase." Password-protected files have been compared to a "locked footlocker inside the bedroom." *Trulock v. Freeh,* 275 F.3d 391, 403 (4th Cir. 2001).

Given the pervasiveness of computers in American homes, this court must reach some, at least tentative, conclusion about the category into which personal computers fall. A personal computer is often a repository for private information the computer's owner does not intend to share with others. . . .

The inquiry into whether the owner of a highly personal object has indicated a subjective expectation of privacy traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked. Determining whether a computer is "locked," or whether a reasonable officer should know a computer may be locked, presents a challenge distinct from that associated with other types of closed containers. Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the "off" position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected "user profile." . . .

Courts addressing the issue of third party consent in the context of computers, therefore, have examined officers' knowledge about password protection as an indication of whether a computer is "locked" in the way a footlocker would be. For example, in *Trulock,* the Fourth Circuit held a live-in girlfriend lacked actual authority to consent to a search of her boyfriend's computer files where the girlfriend told police she and her boyfriend shared the household computer but had separate password-protected files that were inaccessible to the other. The court in that case explained, "Although Conrad had

authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files." . . .

In addition to password protection, courts also consider the location of the computer within the house and other indicia of household members' access to the computer in assessing third party authority. Third party apparent authority to consent to a search has generally been upheld when the computer is located in a common area of the home that is accessible to other family members under circumstances indicating the other family members were not excluded from using the computer. In contrast, where the third party has affirmatively disclaimed access to or control over the computer or a portion of the computer's files, even when the computer is located in a common area of the house, courts have been unwilling to find third party authority.

Andrus' case presents facts that differ somewhat from those in other cases. Andrus' computer was located in a bedroom occupied by the homeowner's fifty-one year old son rather than in a true common area. Dr. Andrus, however, had unlimited access to the room. Law enforcement officers did not ask specific questions about Dr. Andrus' use of the computer, but Dr. Andrus said nothing indicating the need for such questions. *Cf. Trulock,* 275 F.3d at 398 (when law enforcement questioned third party girlfriend about computer, she indicated she and boyfriend had separate password-protected files). The resolution of this appeal turns on whether the officers' belief in Dr. Andrus' authority was reasonable, despite the lack of any affirmative assertion by Dr. Andrus that he used the computer and despite the existence of a user profile indicating Ray Andrus' intent to exclude other household members from using the computer. For the reasons articulated below, this court concludes the officers' belief in Dr. Andrus' authority was reasonable. . . .

First, the officers knew Dr. Andrus owned the house and lived there with family members. Second, the officers knew Dr. Andrus' house had internet access and that Dr. Andrus paid the Time Warner internet and cable bill. Third, the officers knew the email address bandrus@kc.rr.com had been activated and used to register on a website that provided access to child pornography. Fourth, although the officers knew Ray Andrus lived in the center bedroom, they also knew that Dr. Andrus had access to the room at will. Fifth, the officers saw the computer in plain view on the desk in Andrus' room and it appeared available for use by other household members. Furthermore, the record indicates Dr. Andrus did not say or do anything to indicate his lack of ownership or control over the computer when Cheatham asked for his consent to conduct a computer search. It is uncontested that Dr. Andrus led the officers to the bedroom in which the computer was located, and, even after he saw Kanatzar begin to work on the computer, Dr. Andrus remained silent about any lack of authority he had over the computer. Even if Ray Andrus' computer was protected with a user name and password, there is no indication in the record that the officers knew or had reason to believe such protections were in place.

Andrus argues his computer's password protection indicated his computer was "locked" to third parties, a fact the officers would have known had they asked questions of Dr. Andrus prior to searching the computer. Under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous. In essence, by suggesting the onus was on the officers to ask

about password protection prior to searching the computer, despite the absence of any indication that Dr. Andrus' access to the computer was limited by a password, Andrus necessarily submits there is inherent ambiguity whenever police want to search a household computer and a third party has not affirmatively provided information about his own use of the computer or about password protection. Andrus' argument presupposes, however, that password protection of home computers is so common that a reasonable officer ought to know password protection is likely. Andrus has neither made this argument directly nor proffered any evidence to demonstrate a high incidence of password protection among home computer users. . . .

Viewed under the requisite totality-of-the-circumstances analysis, the facts known to the officers at the time the computer search commenced created an objectively reasonable perception that Dr. Andrus was, at least, *one* user of the computer. That objectively reasonable belief would have been enough to give Dr. Andrus apparent authority to consent to a search. Even if Dr. Andrus had no actual ability to use the computer and the computer was password protected, these mistakes of fact do not negate a determination of Dr. Andrus' apparent authority. In this case, the district court found Agent Cheatham properly halted the search when further conversation with Dr. Andrus revealed he did not use the computer and that Andrus' computer was the only computer in the house. These later revelations, however, have no bearing on the reasonableness of the officers' belief in Dr. Andrus' authority at the outset of the computer search.

McKAY, J., dissenting. This case concerns the reasonable expectation of privacy associated with password-protected computers. In examining the contours of a third party's apparent authority to consent to the search of a home computer, the majority correctly indicates that the extent to which law enforcement knows or should reasonably suspect that password protection is enabled is critical. . . . I take issue with the majority's implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party's access to that password.

The presence of security on Defendant's computer is undisputed. Yet, the majority curiously argues that Defendant's use of password protection is inconsequential because Defendant failed to argue that computer password protection is "commonplace." Of course, the decision provides no guidance on what would constitute sufficient proof of the prevalence of password protection, nor does it explain why the court could not take judicial notice that password protection is a standard feature of operating systems. Despite recognizing the "pervasiveness of computers in American homes," and the fact that the "personal computer is often a repository for private information the computer's owner does not intend to share with others," the majority requires the invocation of magical language in order to give effect to Defendant's subjective intent to exclude others from accessing the computer. . . .

The unconstrained ability of law enforcement to use forensic software such as the EnCase program to bypass password protection without first determining whether such passwords have been enabled does not "exacerbate[]" this

difficulty; rather, it avoids it altogether, simultaneously and dangerously sidestepping the Fourth Amendment in the process. Indeed, the majority concedes that if such protection were "shown to be commonplace, law enforcement's use of forensic software like EnCase . . . may well be subject to question." But the fact that a computer password "lock" may not be *immediately* visible does not render it unlocked. I appreciate that unlike the locked file cabinet, computers have no handle to pull. But, like the padlocked footlocker, computers do exhibit outward signs of password protection: they display boot password screens, username/password log-in screens, and/or screen-saver reactivation passwords.

The fact remains that EnCase's ability to bypass security measures is well known to law enforcement. Here, ICE's forensic computer specialist found Defendant's computer turned off. Without turning it on, he hooked his laptop directly to the hard drive of Defendant's computer and ran the EnCase program. The agents made no effort to ascertain whether such security was enabled prior to initiating the search. . . .

The majority points out that law enforcement "did not ask specific questions" about Dr. Andrus' use of the computer or knowledge of Ray Andrus' use of password protection, but twice criticizes Dr. Andrus' failure to affirmatively disclaim ownership of, control over, or knowledge regarding the computer. Of course, the computer was located in Ray Andrus' very tiny bedroom, but the majority makes no effort to explain how this does not create an ambiguous situation as to ownership.

The burden on law enforcement to identify ownership of the computer was minimal. A simple question or two would have sufficed. Prior to the computer search, the agents questioned Dr. Andrus about Ray Andrus' status as a renter and Dr. Andrus' ability to enter his 51-year-old son's bedroom in order to determine Dr. Andrus' ability to consent to a search of the room, but the agents did not inquire whether Dr. Andrus used the computer, and if so, whether he had access to his son's password. At the suppression hearing, the agents testified that they were not immediately aware that Defendant's computer was the only one in the house, and they began to doubt Dr. Andrus' authority to consent when they learned this fact. The record reveals that, upon questioning, Dr. Andrus indicated that there was a computer in the house and led the agents to Defendant's room. The forensic specialist was then summoned. It took him approximately fifteen to twenty minutes to set up his equipment, yet, bizarrely, at no point during this period did the agents inquire about the presence of any other computers. . . .

Accordingly, in my view, given the case law indicating the importance of computer password protection, the common knowledge about the prevalence of password usage, and the design of EnCase or similar password bypass mechanisms, the Fourth Amendment and the reasonable inquiry rule, mandate that in consent-based, warrantless computer searches, law enforcement personnel inquire or otherwise check for the presence of password protection and, if a password is present, inquire about the consenter's knowledge of that password and joint access to the computer. . . .

NOTES & QUESTIONS

1. ***A Question of Perspective?*** Orin Kerr contends:

> From a virtual user's perspective, the child pornography was hidden to the father; it was behind a password-protected gate. Under these facts, the father couldn't consent to a search because he would lack common authority over it. From a physical perspective, however, the file was present on the hard drive just like all the other information. Under these facts, the father could consent to the search because he had access rights to the machine generally. . . .
>
> Viewed from the physical perspective, the investigators reasonably did not know about the user profile and reasonably believed that the father had rights to consent to that part of the hard drive.[62]

2. ***Checking for Password Protection.*** Was the investigators' belief about the father's authority over the computer reasonable? Should the investigators have asked the father more questions about his use of the computer first? Should they have turned on the machine to see if it was password-protected before hooking up the forensic software? What kinds of incentives does this decision engender for officers doing an investigation?

2. ENCRYPTION

Encryption includes the ability to keep communications secure by concealing the contents of a message. With encryption, even if a communication is intercepted, it still remains secure. Encryption works by translating a message into a code of letters or numbers called "cypher text." The parties to the communication hold a *key*, which consists of the information necessary to translate the code back to the original message, or "plain text." Since ancient times, code-makers have devised cryptographic systems to encode messages. But along with the code-makers arose code-breakers, who were able to figure out the keys to cryptographic systems by, for example, examining the patterns in the encoded messages and comparing them to patterns in a particular language and the frequency of use of certain letters in that language. Today, computers have vastly increased the complexity of encryption.

Encryption presents a difficult trade-off between privacy and surveillance. It is an essential technique to protect the privacy of electronic communications in an age when such communications can so easily be intercepted and monitored. On the other hand, it enables individuals to disguise their communications from detection by law enforcement officials.[63] As Whitfield Diffie and Susan Landau observe:

---

[62] Orin Kerr, *Virtual Analogies, Physical Searches, and the Fourth Amendment,* Volokh Conspiracy, Apr. 26, 2007, http://www.volokh.com/posts/1177562355.shtml.

[63] For more background on encryption, see Simon Singh, *The Code: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (1999); Steven Levy, *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age* (2002); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709 (1995); Robert C. Post, *Encryption Source Code and the First Amendment*, 15 Berkeley Tech. L.J. 713 (2000); A. Michael Froomkin, *The Constitution and Encryption Regulation: Do We Need a "New Privacy"?*, 3 N.Y.U. J. Legis. & Pub. Pol'y 25 (1999).

> The explosion in cryptography and the US government's attempts to control it have given rise to a debate between those who hail the new technology's contribution to privacy, business, and security and those who fear both its interference with the work of police and its adverse effect on the collection of intelligence. Positions have often been extreme. The advocates for unfettered cryptography maintain that a free society depends on privacy to protect freedom of association, artistic creativity, and political discussion. The advocates of control hold that there will be no freedom at all unless we can protect ourselves from criminals, terrorists, and foreign threats. Many have tried to present themselves as seeking to maintain or restore the status quo. For the police, the status quo is the continued ability to wiretap. For civil libertarians, it is the ready availability of conversational privacy that prevailed at the time of the country's founding.[64]

The Clipper Chip. The U.S. government has become increasingly concerned that the growing sophistication of encryption would make it virtually impossible for the government to decrypt. In 1994, the government proposed implementing the "Clipper Chip," a federal encryption standard in which the government would retain a copy of the key in a system called "key escrow." By holding a "spare key," the government could readily decrypt encrypted communications if it desired. The Clipper Chip was strongly criticized, and the government's encryption standard has not been widely used.

Encryption and the First Amendment. In *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), the Sixth Circuit concluded that encryption was protected speech under the First Amendment:

> Much like a mathematical or scientific formula, one can describe the function and design of encryption software by a prose explanation; however, for individuals fluent in a computer programming language, source code is the most efficient and precise means by which to communicate ideas about cryptography.

Junger relied on the reasoning of *Bernstein v. United States Dep't of Justice,* 176 F.3d 1132 (9th Cir. 1999) (opinion withdrawn), where the Ninth Circuit struck down a licensing scheme on encryption source code as a violation of the First Amendment:

> Bernstein has submitted numerous declarations from cryptographers and computer programmers explaining that cryptographic ideas and algorithms are conveniently expressed in source code. . . . [T]he chief task for cryptographers is the development of secure methods of encryption. While the articulation of such a system in layman's English or in general mathematical terms may be useful, the devil is, at least for cryptographers, often in the algorithmic details. By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve. . . .
>
> Thus, cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. . . .

---

[64] Whitfield Diffie & Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (1998).

> In light of these considerations, we conclude that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes. . . .

Orin Kerr takes issue with *Junger*'s holding: "the court viewed source code using the close-up paradigm of what the code looked like, rather than the deeper functional perspective of what the code was actually supposed to do. . . . Just as viewing a Seurat painting from inches away reveals only dots, the *Junger* court's myopic view of source code revealed only communications that looked like speech in form, but lacked the deeper significance required to establish constitutional expression."[65]

Consider *Karn v. United States Dep't of State*, 925 F. Supp. 1 (D.D.C. 1996), where the court came to the contrary conclusion from *Junger*:

> . . . The government regulation at issue here is clearly content-neutral. . . . The defendants are not regulating the export of the diskette because of the expressive content of the comments and or source code, but instead are regulating because of the belief that the combination of encryption source code on machine readable media will make it easier for foreign intelligence sources to encode their communications. . . .
>
> . . . [A] content-neutral regulation is justified . . . if it is within the constitutional power of the government, it "furthers an important or substantial governmental interest," and "the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." . . .
>
> . . . By placing cryptographic products on the ITAR, the President has determined that the proliferation of cryptographic products will harm the United States. . . .
>
> . . . [T]he plaintiff has not advanced any argument that the regulation is "substantially broader than necessary" to prevent the proliferation of cryptographic products. Nor has the plaintiff articulated any present barrier to the spreading of information on cryptography "by any other means" other than those containing encryption source code on machine-readable media. Therefore, the Court holds that the regulation of the plaintiff's diskette is narrowly tailored to the goal of limiting the proliferation of cryptographic products and that the regulation is justified. . . .

Encryption and the Fourth Amendment. Suppose law enforcement officials legally obtain an encrypted communication. Does the Fourth Amendment require a warrant before the government can decrypt an encrypted communication? Consider the following argument by Orin Kerr:

> Encryption is often explained as a lock-and-key system, in which a "key" is used to "lock" plaintext by turning it into ciphertext, and then a "key" is used to "unlock" the ciphertext by turning it into plaintext. We know that locking a container is a common way to create a reasonable expectation of privacy in its contents: the government ordinarily cannot break the lock and search a closed container without a warrant. . . .

---

[65] Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1292-93 (2000).

> When we use a "lock" and "unlock" in the metaphorical sense to denote understanding, however, a lock cannot trigger the rights-based Fourth Amendment. If I tell you a riddle, I do not have a right to stop you from figuring it out. Although figuring out the secret of an inscrutable communication may "unlock" its meaning, the Fourth Amendment cannot regulate such a cognitive discovery. . . .[66]

Encryption and the Fifth Amendment. Can the government compel the production of a private key if it is stored on a personal computer? What if the key is known only to the individual and not stored or recorded?

3. E-MAIL

STEVE JACKSON GAMES, INC. V. UNITED STATES SECRET SERVICE

36 F.3d 457 (5th Cir. 1994)

BARKSDALE, J. Appellant Steve Jackson Games, Incorporated (SJG), publishes books, magazines, role-playing games, and related products. Starting in the mid-1980s, SJG operated an electronic bulletin board system, called "Illuminati" (BBS), from one of its computers. SJG used the BBS to post public information about its business, games, publications, and the role-playing hobby; to facilitate play-testing of games being developed; and to communicate with its customers and free-lance writers by electronic mail (E-mail).

Central to the issue before us, the BBS also offered customers the ability to send and receive private E-mail. Private E-mail was stored on the BBS computer's hard disk drive temporarily, until the addressees "called" the BBS (using their computers and modems) and read their mail. After reading their E-mail, the recipients could choose to either store it on the BBS computer's hard drive or delete it. In February 1990, there were 365 BBS users. Among other uses, appellants Steve Jackson, Elizabeth McCoy, William Milliken, and Steffan O'Sullivan used the BBS for communication by private E-mail. . . . [In addition, Lloyd Blankenship, an employee of Steve Jackson Games, operated a computer bulletin bulletin board system (BBS).] Blankeship had the ability to review, and perhaps delete any data on the BBS.

On February 28, 1990, [Secret Service] Agent Foley applied for a warrant to search SJG's premises and Blankenship's residence for evidence of violations of 18 U.S.C. §§ 1030 (proscribes interstate transportation of computer access information) and 2314 (proscribes interstate transportation of stolen property). A search warrant for SJG was issued that same day, authorizing the seizure of [computer hardware, software, and computer data.]

The next day, March 1, the warrant was executed by the Secret Service, including Agents Foley and Golden. Among the items seized was the computer which operated the BBS. At the time of the seizure, 162 items of unread, private

---

[66] Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 Conn. L. Rev. 503, 520-21, 522 (2001).

E-mail were stored on the BBS, including items addressed to the individual appellants. . . .

Appellants filed suit in May 1991 against, among others, the Secret Service and the United States, claiming [among other things, a violation of] the Federal Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2521; and Title II of the ECPA, 18 U.S.C. §§ 2701-2711. . . .

As stated, the sole issue is a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. § 2511(1)(a).

Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications. In relevant part, § 2511(1)(a) proscribes "intentionally intercept[ing] . . . any wire, oral, or electronic communication," unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, *inter alia*, persons whose electronic communications are intercepted in violation of § 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater. 18 U.S.C. § 2520.

The Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). . . .

Webster's Third New International Dictionary (1986) defines "aural" as "of or relating to the ear" or "of or relating to the sense of hearing." And, the Act defines "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18). This definition is extremely important for purposes of understanding the definition of a "wire communication," which is defined by the Act as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) . . . *and such term includes any electronic storage of such communication.*

18 U.S.C. § 2510(1) (emphasis added). In contrast, as noted, an "electronic communication" is defined as "any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does not include . . . any wire or oral communication. . . ." 18 U.S.C. § 2510(12) (emphasis added).

Critical to the issue before us is the fact that, unlike the definition of "wire communication," *the definition of "electronic communication" does not include electronic storage of such communications. See* 18 U.S.C. § 2510(12). "Electronic storage" is defined as

> (A) any *temporary*, intermediate *storage* of a wire or *electronic communication incidental to the electronic transmission thereof;* and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. . . .

18 U.S.C. § 2510(17) (emphasis added). The E-mail in issue was in "electronic storage." Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication" (part of the definition of "wire communication") reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage." . . .

Title II generally proscribes unauthorized access to stored wire or electronic communications. Section 2701(a) provides:

> Except as provided in subsection (c) of this section whoever —
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication *while it is in electronic storage in such system* shall be punished. . . .

18 U.S.C. § 2701(a) (emphasis added).

As stated, the district court found that the Secret Service violated § 2701 when it

> intentionally accesse[d] without authorization a facility [the computer] through which an electronic communication service [the BBS] is provided . . . and thereby obtain[ed] [and] prevent[ed] authorized access [by appellants] to a[n] . . . electronic communication while it is in electronic storage in such system.

18 U.S.C. § 2701(a). The Secret Service does not challenge this ruling. We find no indication in either the Act or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I as well. . . .

NOTES & QUESTIONS

1. ***Interception vs. Electronic Storage.*** Is unread e-mail in storage because it is sitting on a hard drive at the ISP? Or is it in transmission because the recipient hasn't read it yet? Is the court applying an overly formalistic and strict reading of "interception"?
2. ***The Fourth Amendment and E-mail: A Question of Perspective?*** Suppose the police sought to obtain a person's unread e-mail messages that were stored with her ISP waiting to be downloaded. *Steve Jackson Games* demonstrates how ECPA would apply — the weaker provisions of the Stored Communications Act rather than the stronger protections of the Wiretap Act apply to e-mail temporarily stored with a person's ISP. *Steve Jackson Games* is a civil case. In the criminal law context, the Stored Communications Act requires a warrant to obtain e-mails stored at the ISP for 180 days or less. If the e-mails

have been stored over 180 days, then the government can obtain them with a mere subpoena.

Would the Fourth Amendment apply? Orin Kerr argues that the answer depends upon the perspective by which one views the Internet. In the "internal perspective," the Internet is viewed as a virtual world, analogous to real space. From the "external perspective," we view the Internet as a network and do not analogize to real space. Kerr provides the following example:

> Does the Fourth Amendment require [the police] to obtain a search warrant [to obtain an e-mail]? . . . The answer depends largely upon whether they apply an internal or external perspective of the Internet.
>
> Imagine that the first officer applies an internal perspective of the Internet. To him, e-mail is the cyberspace equivalent of old-fashioned postal mail. His computer announces, "You've got mail!" when an e-mail message arrives and shows him a closed envelope. When he clicks on the envelope, it opens, revealing the message. From his internal perspective, the officer is likely to conclude that the Fourth Amendment places the same restriction on government access to e-mail that it places on government access to ordinary postal mail. He will then look in a Fourth Amendment treatise for the black letter rule on accessing postal mail. That treatise will tell him that accessing a suspect's mail ordinarily violates the suspect's "reasonable expectation of privacy," and that therefore the officer must first obtain a warrant. Because e-mail is the equivalent of postal mail, the officer will conclude that the Fourth Amendment requires him to obtain a warrant before he can access the e-mail.
>
> Imagine that the second police office approaches the same problem from an external perspective. To him, the facts look quite different. Looking at how the Internet actually works, the second police officer sees that when A sent the e-mail to B, A was instructing his computer to send a message to his Internet Service Provider (ISP) directing the ISP to forward a text message to B's ISP. To simplify matters, let's say that A's ISP is EarthLink, and B's ISP is America Online (AOL). . . .
>
> What process does the Fourth Amendment require? The second officer will reason that A sent a copy of the e-mail communication to a third party (the EarthLink computer), disclosing the communication to the third party and instructing it to send the communication to yet another third party (AOL). The officer will ask, what process does the Fourth Amendment require to obtain information that has been disclosed to a third party and is in the third party's possession? The officer will look in a Fourth Amendment treatise and locate to the black letter rule that the Fourth Amendment permits the government to obtain information disclosed to a third party using a mere subpoena. The officer can simply subpoena the system administrator to compel him to produce the e-mails. No search warrant is required.
>
> Who is right? The first officer or the second? The answer depends on whether you approach the Internet from an internal or external perspective. From an internal perspective, the officers need a search warrant; from the external perspective, they do not.[67]

[67] Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 Geo. L.J. 357, 361-62, 365-67 (2003).

3. ***Previously Read E-mail Stored at an ISP.*** The e-mail stored on the ISP server in *Steve Jackson Games* had not yet been downloaded and read by the recipients. Many people continue to store their e-mail messages with their ISP even after having read them. Does the Stored Communications Act protect them in the same way? The answer to this question is currently in dispute. Daniel Solove observes:

> Because these messages are now stored indefinitely, according to the DOJ's interpretation . . . the e-mail is no longer in temporary storage and is "simply a remotely stored file." Therefore, under this view, it falls outside of much of the Act's protections. Since many people store their e-mail messages after reading them and the e-mail they send out, this enables the government to access their communications with very minimal limitations.[68]

In *Theofel v. Farey-Jones,* 359 F.3d 1066 (9th Cir. 2004), the court concluded that

> [t]he [Stored Communications] Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Id. § 2510(17), incorporated by id. § 2711(1). Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient. Because subsection (A) applies only to messages in "temporary, intermediate storage," however, these courts have limited that subsection's coverage to messages not yet delivered to their intended recipient.
>
> Defendants point to these cases and argue that messages remaining on an ISP's server after delivery no longer fall within the Act's coverage. But, even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B). . . .
>
> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again — if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

See also Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 108 (3d Cir. 2003) (suggesting that such e-mail messages were in backup storage under the definition of electronic storage).

4. ***What Constitutes an Interception?*** In *United States v. Councilman,* 373 F.3d 197 (1st Cir. 2004), an Internet bookseller, Interloc, Inc., provided e-mail service for its customers, who were book dealers. Councilman, the vice president of Interloc, directed Interloc employees to draft a computer program to intercept all incoming communications from Amazon.com to the book dealers and make copies of them. Councilman and other Interloc then read the

---

[68] Daniel J. Solove, *Reconstructing Electronic Surveillance Law,* 72 Geo. Wash. L. Rev. 1264 (2004).

e-mails in order to gain a commercial advantage. Councilman was charged with criminal violations of the Wiretap Act. Councilman argued that he did not violate the Wiretap Act because the e-mails were in electronic storage, albeit very briefly, when they were copied. The court followed *Steve Jackson Games* and concluded that the e-mail was in temporary storage and therefore subject to the Stored Communications Act, not the Wiretap Act. However, unlike *Steve Jackson Games,* Interloc accessed the e-mails "as they were being transmitted and in real time."

The *Councilman* case received significant criticism by academic commentators and experts in electronic surveillance law for misunderstanding the fundamental distinction between the interception of a communication and the accessing of a stored communication. An interception occurs contemporaneously — as the communication is being transmitted. Accessing a stored communication occurs later, as the communication sits on a computer. This distinction has practical consequences, since interceptions are protected by the much more protective Wiretap Act rather than the Stored Communications Act. Does such a distinction still make sense? Is the contemporaneous interception of communications more troublesome than the accessing of the communications in *Steve Jackson Games*?

The case was reheard en banc, and the en banc court reversed the panel. *See United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc). The court concluded that "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act." The court declined to further elaborate on what constitutes and "interception."

5. ***Carnivore.*** Beginning in 1998, the FBI began using a hardware and software mechanism called "Carnivore" to intercept people's e-mail and instant messaging information from their Internet Service Providers (ISPs). After obtaining judicial authorization, the FBI would install Carnivore by connecting a computer directly to the ISP's server and initiating the program. Carnivore was designed to locate the e-mails of a suspect at the ISP when the ISP did not have the capacity to do so.

   Carnivore was capable of analyzing the entire e-mail traffic of an ISP, although the FBI maintained it was only used to search for the e-mails of a suspect. The program filtered out the e-mail messages of ISP subscribers who are not the subject of the investigation; but to do so, it had to scan the e-mail headers that identify the senders and recipients. The FBI likened e-mail headers to the information captured by a pen register, a device that registers the phone numbers a person dials.

   However, Carnivore could be programmed to search through the entire text of all e-mails, to capture e-mails with certain key words. In this way, Carnivore resembles a wiretap. Recall that under federal wiretap law, judicial approval for obtaining pen register information only requires a certification that "the information likely to be obtained by such installation and use is relevant to an ongoing investigation." 18 U.S.C. § 3123. In contrast, judicial

approval of a wiretap requires a full panoply of requirements under Title I, including a showing of probable cause.

To eliminate the negative associations with the term "Carnivore," the device was renamed "DCS1000." Many members of Congress viewed Carnivore with great suspicion. Congress held hearings over the summer of 2000 pertaining to Carnivore, and several bills were proposed to halt or limit the use of Carnivore.

The anti-Carnivore sentiment abruptly ended after the September 11, 2001, World Trade Center and Pentagon terrorist attacks. Section 216 of the USA PATRIOT Act of 2001, in anticipation of the use of Carnivore, required reports on the use of Carnivore to be filed with a court. These reports, filed under seal, require (1) the names of the officers using the device; (2) when the device was installed, used, and removed; (3) the configuration of the device; and (4) the information collected by the device. 18 U.S.C. § 3133(a)(3).

The FBI discontinued use of Carnivore because ISPs can readily produce the information the FBI desires without the assistance of the Carnivore device and because commercially available software has similar functionality.

4. ISP RECORDS

UNITED STATES V. HAMBRICK

55 F. Supp. 2d 504 (W.D. Va. 1999)

MICHAEL, J. Defendant Scott M. Hambrick seeks the suppression of all evidence obtained from his Internet Service Provider ("ISP"), MindSpring, and seeks the suppression of all evidence seized from his home pursuant to a warrant issued by this court. For the reasons discussed below, the court denies the defendant's motion.

On March 14, 1998, J. L. McLaughlin, a police officer with the Keene, New Hampshire Police Department, connected to the Internet and entered a chat room called "Gay dads 4 sex." McLaughlin's screen name was "Rory14." In this chat room, Detective McLaughlin encountered someone using the screen name "Blowuinva." Based on a series of online conversations between "Rory14" (Det. McLaughlin) and "Blowuinva," McLaughlin concluded that "Blowuinva" sought to entice a fourteen-year-old boy to leave New Hampshire and live with "Blowuinva." Because of the anonymity of the Internet, Detective McLaughlin did not know the true identity of the person with whom he was communicating nor did he know where "Blowuinva" lived. "Blowuinva" had only identified himself as "Brad."

To determine Blowuinva's identity and location, McLaughlin obtained a New Hampshire state subpoena that he served on Blowuinva's Internet Service Provider, MindSpring, located in Atlanta, Georgia. The New Hampshire state subpoena requested that MindSpring produce "any records pertaining to the billing and/or user records documenting the subject using your services on March 14th, 1998 at 1210HRS (EST) using Internet Protocol Number 207.69.169.92." MindSpring complied with the subpoena. On March 20, 1998, MindSpring

supplied McLaughlin with defendant's name, address, credit card number, e-mail address, home and work telephone numbers, fax number, and the fact that the Defendant's account was connected to the Internet at the Internet Protocol (IP) address.

A justice of the peace, Richard R. Richards, signed the New Hampshire state subpoena. Mr. Richards is not only a New Hampshire justice of the peace, but he is also a detective in the Keene Police Department, Investigation Division. Mr. Richards did not issue the subpoena pursuant to a matter pending before himself, any other judicial officer, or a grand jury. At the hearing on the defendant's motion, the government conceded the invalidity of the warrant. The question before this court, therefore, is whether the court must suppress the information obtained from MindSpring, and all that flowed from it, because the government failed to obtain a proper subpoena. . . .

. . . [Under *Katz v. United States*,] the Fourth Amendment applies only where: (1) the citizen has manifested a subjective expectation of privacy, and (2) the expectation is one that society accepts as "objectively reasonable." . . . Applying the first part of the *Katz* analysis, Mr. Hambrick asserts that he had a subjective expectation of privacy in the information that MindSpring gave to the government. However, resolution of this matter hinges on whether Mr. Hambrick's expectation is one that society accepts as "objectively reasonable."

The objective reasonableness prong of the privacy test is ultimately a value judgment and a determination of how much privacy we should have as a society. In making this constitutional determination, this court must employ a sort of risk analysis, asking whether the individual affected should have expected the material at issue to remain private. The defendant asserts that the Electronic Communications Privacy Act ("ECPA") "legislatively resolves" this question. . . .

The information obtained through the use of the government's invalid subpoena consisted of the defendant's name, address, social security number, credit card number, and certification that the defendant was connected to the Internet on March 14, 1998. Thus, this information falls within the provisions of Title II of the ECPA.

The government may require that an ISP provide stored communications and transactional records only if (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question. *See* 18 U.S.C. § 2703(a)-(c)(1)(B). When an ISP discloses stored communications or transactional records to a government entity without the requisite authority, the aggrieved customer's sole remedy is damages.

Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of "reasonably objective" for Fourth Amendment purposes. Despite its concern for privacy, Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act. Additionally, the ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental entities. *See* 18 U.S.C. § 2703(c)(1)(A) ("[A] provider

of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service . . . to any person other than a governmental entity."). For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information. This, however, does not end the court's inquiry. This court must determine, within the constitutional framework that the Supreme Court has established, whether Mr. Hambrick's subjective expectation of privacy is one that society is willing to recognize.

To have any interest in privacy, there must be some exclusion of others. To have a reasonable expectation of privacy under the Supreme Court's risk-analysis approach to the Fourth Amendment, two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure. In *Katz*, the Supreme Court expressly held that "what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection." Further, the Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). . . .

When Scott Hambrick surfed the Internet using the screen name "Blowuinva," he was not a completely anonymous actor. It is true that an average member of the public could not easily determine the true identity of "Blowuinva." Nevertheless, when Mr. Hambrick entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees. Mr. Hambrick also selected the screen name "Blowuinva." When the defendant selected his screen name it became tied to his true identity in all MindSpring records. MindSpring employees had ready access to these records in the normal course of MindSpring's business, for example, in the keeping of its records for billing purposes, and nothing prevented MindSpring from revealing this information to nongovernmental actors.[69] Also, there is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant's personal information to nongovernmental entities. Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.

Although not dispositive to the outcome of this motion, it is important to note that the court's decision does not leave members of cybersociety without privacy protection. Under the ECPA, Internet Service Providers are civilly liable when they reveal subscriber information or the contents of stored communications to

[69] It is apparently common for ISPs to provide certain information that Mr. Hambrick alleges to be private to marketing firms and other organizations interested in soliciting business from Internet users.

the government without first requiring a warrant, court order, or subpoena. Here, nothing suggests that MindSpring had any knowledge that the facially valid subpoena submitted to it was in fact an invalid subpoena. Had MindSpring revealed the information at issue in this case to the government without first requiring a subpoena, apparently valid on its face, Mr. Hambrick could have sued MindSpring. This is a powerful deterrent protecting privacy in the online world and should not be taken lightly. . . .

NOTES & QUESTIONS

1. ***Is There a Reasonable Expectation of Privacy in ISP Records?*** The court in *Hambrick* concludes that there is no reasonable expectation of privacy in ISP records based on the third party doctrine in *Smith v. Maryland.* In *United States v. Kennedy,* 81 F. Supp. 2d 1103 (D. Kan. 2000), the court reached a similar conclusion:

> Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information. . . . "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland,* 442 U.S. 735 (1979). When defendant entered into an agreement with [his ISP], he knowingly revealed all information connected to [his IP address]. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information.

   Is *Smith v. Maryland* controlling on this issue? Is there a way to distinguish *Smith*?

2. ***Statutes as a Basis for a Reasonable Expectation of Privacy?*** Hambrick was not seeking relief directly under the Stored Communications Act of ECPA. Why not? Instead, Hambrick asserted he had Fourth Amendment protection in his subscriber records. He argued that under the *Katz* reasonable expectation of privacy test, the ECPA "legislatively resolves" that there is a reasonable expectation of privacy in information that Mindspring gave to the government. Should statutes that protect privacy serve as an indication of a societal recognition of a reasonable expectation of privacy? What are the consequences of using statutes such as ECPA to conclude that the Fourth Amendment applies?
3. ***Is There a Remedy?*** Mindspring couldn't release information to the government without a warrant or subpoena or else it would face civil liability. However, in this case, the government presented Mindspring with a subpoena that Mindspring had no knowledge was invalid. Therefore, it is unlikely that Mindspring would be liable. If the court is correct in its conclusion that 18 U.S.C. § 2703(a)–(c)(1)(B) of the ECPA only applies to the conduct of Internet Service Providers, then is there any remedy against Officer Richards's blatantly false subpoena? Could a police officer obtain a person's Internet subscriber information by falsifying a subpoena and escape without any civil liability or exclusionary rule?

5. IP ADDRESSES AND URLS

UNITED STATES V. FORRESTER

512 F.3d 500 (9th Cir. 2008)

FISHER, J. . . . Defendants-appellants Mark Stephen Forrester and Dennis Louis Alba were charged with various offenses relating to the operation of a large Ecstasy-manufacturing laboratory, and were convicted on all counts following a jury trial. They now appeal their convictions and sentences. . . .

During its investigation of Forrester and Alba's Ecstasy-manufacturing operation, the government employed various computer surveillance techniques to monitor Alba's e-mail and Internet activity. The surveillance began in May 2001 after the government applied for and received court permission to install a pen register analogue known as a "mirror port" on Alba's account with PacBell Internet. The mirror port was installed at PacBell's connection facility in San Diego, and enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account. Later, the government obtained a warrant authorizing it to employ imaging and keystroke monitoring techniques, but Alba does not challenge on appeal those techniques' legality or the government's application to use them.

Forrester and Alba were tried by jury. At trial, the government introduced extensive evidence showing that they and their associates built and operated a major Ecstasy laboratory. . . .

Alba contends that the government's surveillance of his e-mail and Internet activity violated the Fourth Amendment and fell outside the scope of the then-applicable federal pen register statute. We hold that the surveillance did not constitute a Fourth Amendment search and thus was not unconstitutional. We also hold that whether or not the computer surveillance was covered by the then-applicable pen register statute — an issue that we do not decide — Alba is not entitled to the suppression of any evidence (let alone the reversal of his convictions) as a consequence.

The Supreme Court held in *Smith v. Maryland* that the use of a pen register (a device that records numbers dialed from a phone line) does not constitute a search for Fourth Amendment purposes. According to the Court, people do not have a subjective expectation of privacy in numbers that they dial because they "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Even if there were such a subjective expectation, it would not be one that society is prepared to recognize as reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Therefore the use of a pen register is not a Fourth Amendment search. Importantly, the Court distinguished pen registers from more intrusive

surveillance techniques on the ground that "pen registers do not acquire the *contents* of communications" but rather obtain only the addressing information associated with phone calls.

Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account. We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith.* First, e-mail and Internet users, like the telephone users in *Smith,* rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.

Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses — but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.[70]

---

[70] Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed.

The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. E-mail, like physical mail, has an outside address "visible" to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not. . . .

We therefore hold that the computer surveillance techniques that Alba challenges are not Fourth Amendment searches. However, our holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register. . . .

Alba claims that the government's computer surveillance was not only unconstitutional but also beyond the scope of the then-applicable pen register statute, 18 U.S.C. § 3121-27 (amended October 2001). Under both the old and new versions of 18 U.S.C. § 3122, the government must apply for and obtain a court order before it can install and use a pen register. When the surveillance at issue here took place in May-July 2001, the applicable statute defined a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3). Notwithstanding the government's invocation of this provision and application for and receipt of a court order, Alba maintains that the computer surveillance at issue here did not come within the statutory definition of a "pen register."

Even assuming that Alba is correct in this contention, he would not be entitled to the suppression of the evidence obtained through the computer surveillance. As both the Supreme Court and this court have emphasized, suppression is a disfavored remedy, imposed only where its deterrence benefits outweigh its substantial social costs or (outside the constitutional context) where it is clearly contemplated by the relevant statute. . . . Alba does not point to any statutory language requiring suppression when computer surveillance that is similar but not technically equivalent to a pen register is carried out. Indeed, he does not even identify what law or regulation the government may have violated if its surveillance did not come within the scope of the then-applicable pen register statute. The suppression of evidence under these circumstances is plainly inappropriate.

Our conclusion is bolstered by the fact that suppression still would not be appropriate even if the computer surveillance was covered by the pen register statute. Assuming the surveillance violated the statute, there is no mention of suppression of evidence in the statutory text. Instead, the only penalty specified is that "[w]hoever knowingly violates subsection (a)" by installing or using a pen register without first obtaining a court order "shall be fined under this title or imprisoned not more than one year, or both." 18 U.S.C. § 3121(d).

NOTES & QUESTIONS

1. ***IP Addresses vs. URLs.*** The *Forrester* court concludes that e-mail headers and IP addresses are akin to pen registers and that the controlling case is *Smith v. Maryland.* Does *Smith* control because IP address and e-mail header information are not revealing of the contents of the communications or because this information is conveyed to a third party? Recall that in a footnote, the court observes that URLs "might be more constitutionally problematic" because a "URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity." However, although IP addresses do not reveal specific parts of a websites that a person visits, they do reveal the various websites that a person visits. Why isn't this revealing enough to trigger constitutional protections?
2. ***Content vs. Envelope Information.*** A key distinction under ECPA, as well as Fourth Amendment law, is between "content" and "envelope" information. Orin Kerr explains the distinction:

> . . . [E]very communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications. The former is "content information," and the latter is "envelope information."
>
> The essential distinction between content and envelope information remains constant across different technologies, from postal mail to email. With postal mail, the content information is the letter itself, stored safely inside its envelope. The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.
>
> Similar distinctions exist for telephone conversations. The content information for a telephone call is the actual conversation between participants that can be captured by an audio recording of the call. The envelope information includes the number the caller dials, the number from which the caller dials, the time of the call, and its duration.[71]

Under ECPA, content information is generally given strong protection (e.g., the Wiretap Act), whereas envelope information is not (e.g., the Pen Register Act). But is such a distinction viable?

Daniel Solove contends that the distinction breaks down:

> When applied to IP addresses and URLs, the envelope/content distinction becomes even more fuzzy. An IP address is a unique number that is assigned to each computer connected to the Internet. Each website, therefore, has an IP address. On the surface, a list of IP addresses is simply a list of numbers; but it is actually much more. With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on.

---

[71] Orin S. Kerr, Internet *Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't,* 97 Nw. U. L. Rev. 607, 611 (2003).

> Perhaps even more revealing are URLs. A URL is a pointer — it points to the location of particular information on the Internet. In other words, it indicates where something is located. When we cite to something on the Web, we are citing to its URL. . . . URLs can reveal the specific information that people are viewing on the Web. URLs can also contain search terms. . . .
>
> [Therefore,] the content/envelope distinction is not always clear. In many circumstances, to adapt Marshall McLuhan, the "envelope" *is* the "content." Envelope information can reveal a lot about a person's private activities, sometimes as much (and even more) than can content information.[72]

Orin Kerr disagrees:

> Professor Solove appears to doubt the wisdom of offering lower privacy protection for non-content information. He suggests that the acquisition of non-content information should require a full search warrant based on probable cause. . . .
>
> Despite this, Solove's suggestion that the law should not offer lesser privacy protection for non-content information is unpersuasive. The main reason is that it is quite rare for non-content information to yield the equivalent of content information. It happens in very particular circumstances, but it remains quite rare, and usually in circumstances that are difficult to predict ex ante. In the Internet context, for example, non-content surveillance typically consists of collecting Internet packets; the packets disclose that a packet was sent from one IP address to another IP address at a particular time. This isn't very private information, at least in most cases. Indeed, it is usually impossible to know who asked for the packet, or what the packet was about, or what the person who asked for the packet wanted to do, or even if it was a person (as opposed to the computer) who sent for the packet in the first place. Solove focuses on the compelling example of Internet search terms as an example of non-content information that can be the privacy equivalent of content information. This is a misleading example, however, as Internet search terms very well may be contents. . . . Thus, despite the fact that non-content information can yield private information, in the great majority of cases contents of communications implicate privacy concerns on a higher order of magnitude than non-content information, and it makes sense to give greater privacy protections for the former and lesser to the latter.[73]

Solove replies:

> Kerr assumes that a compilation of envelope information is generally less revealing than content information. However, a person may care more about protecting the identities of people with whom she communicates than the content of those communications. Indeed, the identities of the people one communicates with implicates freedom of association under the First Amendment. The difficulty is that the distinction between content and envelope information does not correlate well to the distinction between sensitive and innocuous information. Envelope information can be quite sensitive; content information can be quite innocuous. Admittedly, in many cases, people do not care very much about maintaining privacy over the identities of their friends and

---

[72] Solove, *Surveillance Law, supra*, at 1287-88.

[73] Orin S. Kerr, *A User's Guide to the Stored Communications Act — and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208, 1229 n.142 (2004).

> associates. But it is also true that in many cases, the contents of communications are not very revealing as well. Many e-mails are short messages which do not reveal any deep secrets, and even Kerr would agree that this should not lessen their protection under the law. This is because content information has the potential to be quite sensitive — but this is also the case with envelope information.[74]

3. ***The Scope of the Pen Register Act.*** The version of the Pen Register Act in effect when the search took place in *Forrester* was the pre-USA PATRIOT Act version, which defined pen registers more narrowly as "numbers dialed." The USA PATRIOT Act expanded the definition of pen register to include "dialing, routing, addressing, or signaling information . . . provided, however, that such information shall not include the contents of any communication." Prior to the USA PATRIOT Act changes, it was an open question as to whether the Pen Register Act applied to e-mail headers, IP addresses, and URLs. The USA PATRIOT Act changes aimed to clarify that the Pen Register Act did apply beyond telephone numbers. E-mail headers seem to fit readily into the new Pen Register Act definition. But what about IP addresses and URLs? They involve "routing" and "addressing" information, but they may also include "the contents" of communications. Do they involve "contents" or are they merely "envelope" information?
4. ***Text Messages.*** In *Quon v. Arch Wireless Operating Co., Ltd.*, 2008 WL 2440559 (9th Cir. 2008), the court held that accessing text messages can constitute a violation of the Stored Communications Act because the messages were stored by the communication service provider as "backup" protection for the user. The court also concluded that the Fourth Amendment protects text message communications because they are "content" information: "We see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here."
5. ***ECPA and the Exclusionary Rule.*** The *Forrester* court concludes that even if the acquisition of information violated the Pen Register Act, the exclusionary rule is not a remedy under the Act. As discussed earlier in this chapter, many provisions of electronic surveillance law lack an exclusionary rule. In the Wiretap Act, wire and oral communications are protected with an exclusionary rule, but electronic communications are not. Solove argues that "[s]ince e-mail has become a central mode of communication, this discrepancy is baseless."[75] Is it? Can you think of a reason why e-mail should receive lesser protection than a phone conversation, which would be protected by the exclusionary rule under the Wiretap Act? Additionally, the Stored Communications Act and Pen Register Act have no exclusionary remedies for any type of communication.

---

[74] Solove, *Surveillance Law, supra,* at 1288. Susan Freiwald contends that "the current categories of the ECPA do not cover web traffic data. At least one other category of protection is needed. Search terms entered, web-pages visited, and items viewed are neither message contents nor their to/from information." Freiwald, *Online Surveillance, supra,* at 71.

[75] Solove, *Surveillance Law, supra*, at 1282.

Orin Kerr argues the absence of an exclusionary rule in many of ECPA's provisions leads to inadequate judicial attention to ECPA. Without an exclusionary rule, Kerr contends, "criminal defendants have little incentive to raise challenges to the government's Internet surveillance practices." Therefore, many challenges to Internet surveillance practices "tend to be in civil cases between private parties that raise issues far removed from those that animated Congress to pass the statutes." Adding an exclusionary remedy, Kerr argues, would "benefit both civil libertarian and law enforcement interests alike." He writes:

> On the civil libertarian side, a suppression remedy would considerably increase judicial scrutiny of the government's Internet surveillance practices in criminal cases. The resulting judicial opinions would clarify the rules that the government must follow, serving the public interest of greater transparency. Less obviously, the change could also benefit law enforcement by altering the type and nature of the disputes over the Internet surveillance laws that courts encounter. Prosecutors would have greater control over the types of cases the courts decided, enjoy more sympathetic facts, and have a better opportunity to explain and defend law enforcement interests before the courts. The statutory law of Internet surveillance would become more like the Fourth Amendment law: a source of vital and enforceable rights that every criminal defendant can invoke, governed by relatively clear standards that by and large respect law enforcement needs and attempt to strike a balance between those needs and privacy interests.[76]

6. ***The Internet vs. the Telephone.*** Susan Freiwald contends that while the 1968 Wiretap Act (Title III) provided powerful and effective protection for telephone communications, ECPA in 1986 did not do the same for online communications:

> . . . [O]nline surveillance is even more susceptible to law enforcement abuse and even more threatening to privacy. Therefore, one might expect regulation of online surveillance to be more privacy-protective than traditional wiretapping law. That could not be further from the truth. The law provides dramatically less privacy protection for online activities than for traditional telephone calls and videotapings. Additionally, what makes the Wiretap Act complex makes online surveillance law chaotic. Almost all of the techniques designed to rein in law enforcement have been abandoned in the online context. And, while Congress resolved much of its ambivalence towards wiretapping in 1968, current law suggests the outright hostility of all branches of government to online privacy.[77]

In what ways does federal electronic surveillance law protect Internet communication differently from telephone communication? Should the privacy protections differ in these areas?

---

[76] Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805, 824, 807-08 (2003).

[77] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 14 (2004).

6. KEY LOGGING DEVICES

UNITED STATES v. SCARFO

180 F. Supp. 2d 572 (D.N.J. 2001)

POLITAN, J. . . . Acting pursuant to federal search warrants, the F.B.I. on January 15, 1999, entered Scarfo and Paolercio's business office, Merchant Services of Essex County, to search for evidence of an illegal gambling and loansharking operation. During their search of Merchant Services, the F.B.I. came across a personal computer and attempted to access its various files. They were unable to gain entry to an encrypted file named "Factors."

Suspecting the "Factors" file contained evidence of an illegal gambling and loansharking operation, the F.B.I. returned to the location and, pursuant to two search warrants, installed what is known as a "Key Logger System" ("KLS") on the computer and/or computer keyboard in order to decipher the passphrase to the encrypted file, thereby gaining entry to the file. The KLS records the keystrokes an individual enters on a personal computer's keyboard. The government utilized the KLS in order to "catch" Scarfo's passphrases to the encrypted file while he was entering them onto his keyboard. Scarfo's personal computer features a modem for communication over telephone lines and he possesses an America Online account. The F.B.I. obtained the passphrase to the "Factors" file and retrieved what is alleged to be incriminating evidence.

On June 21, 2000, a federal grand jury returned a three count indictment against the Defendants charging them with gambling and loansharking. The Defendant Scarfo then filed his motion for discovery and to suppress the evidence recovered from his computer. After oral argument was heard on July 30, 2001, the Court ordered additional briefing by the parties. In an August 7, 2001, Letter Opinion and Order, this Court expressed serious concerns over whether the government violated the wiretap statute in utilizing the KLS on Scarfo's computer. Specifically, the Court expressed concern over whether the KLS may have operated during periods when Scarfo (or any other user of his personal computer) was communicating via modem over telephone lines, thereby unlawfully intercepting wire communications without having applied for a wiretap pursuant to Title III, 18 U.S.C. § 2510.

As a result of these concerns, on August 7, 2001, this Court ordered the United States to file with the Court a report explaining fully how the KLS device functions and describing the KLS technology and how it works vis-à-vis the computer modem, Internet communications, e-mail and all other uses of a computer. In light of the government's grave concern over the national security implications such a revelation might raise, the Court permitted the United States to submit any additional evidence which would provide particular and specific reasons how and why disclosure of the KLS would jeopardize both ongoing and future domestic criminal investigations and national security interests.

The United States responded by filing a request for modification of this Court's August 7, 2001, Letter Opinion and Order so as to comply with the procedures set forth in the Classified Information Procedures Act, Title 18, United States Code, Appendix III, § 1 *et seq.* ("CIPA"). [The FBI contended that

a detailed disclosure of how the KLS worked would negatively affect national security and that this information was classified. After an in camera, ex parte hearing with several officials from the Attorney General's office and the FBI, the court granted the government's request not to release the details of how KLS functioned. Instead, the government would provide Scarfo and his attorneys with an unclassified summary about how KLS worked. Based on that summary, Scarfo contended that the KLS violated the Fourth Amendment because the KLS had the capability of collecting data on all of his keystrokes, not merely those of his passphrase.]

Where a search warrant is obtained, the Fourth Amendment requires a certain modicum of particularity in the language of the warrant with respect to the area and items to be searched and/or seized. The particularity requirement exists so that law enforcement officers are constrained from undertaking a boundless and exploratory rummaging through one's personal property. . . . Because the encrypted file could not be accessed via traditional investigative means, Judge Haneke's Order permitted law enforcement officers to "install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on Nicodemo S. Scarfo's computer in the TARGET LOCATION so that the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered." The Order also allowed the F.B.I. to

> search for and seize business records in whatever form they are kept (e.g., written, mechanically or computer maintained and any necessary computer hardware, including computers, computer hard drives, floppy disks or other storage disks or tapes as necessary to access such information, as well as, seizing the mirror hard drive to preserve configuration files, public keys, private keys, and other information that may be of assistance in interpreting the password) — including address and telephone books and electronic storage devices; ledgers and other accounting-type records; banking records and statements; travel records; correspondence; memoranda; notes; calendars; and diaries — that contain information about the identities and whereabouts of conspirators, betting customers and victim debtors, and/or that otherwise reveal the origin, receipt, concealment or distribution of criminal proceeds relating to illegal gambling, loansharking and other racketeering offenses.

On its face, the Order is very comprehensive and lists the items, including the evidence in the encrypted file, to be seized with more than sufficient specificity. *See Andresen v. Maryland,* 427 U.S. 463, 480-81 (1976) (defendant's general warrant claim rejected where search warrant contained, among other things, a lengthy list of specified and particular items to be seized). One would be hard pressed to draft a more specified or detailed search warrant than the May 8, 1999 Order. Indeed, it could not be written with more particularity. It specifically identifies each piece of evidence the F.B.I. sought which would be linked to the particular crimes the F.B.I. had probable cause to believe were committed. Most importantly, Judge Haneke's Order clearly specifies the key piece of the puzzle the F.B.I. sought — Scarfo's passphrase to the encrypted file.

That the KLS certainly recorded keystrokes typed into Scarfo's keyboard *other* than the searched-for passphrase is of no consequence. This does not, as Scarfo argues, convert the limited search for the passphrase into a general

exploratory search. During many lawful searches, police officers may not know the exact nature of the incriminating evidence sought until they stumble upon it. Just like searches for incriminating documents in a closet or filing cabinet, it is true that during a search for a passphrase "some innocuous [items] will be at least cursorily perused in order to determine whether they are among those [items] to be seized."

Hence, "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision." Where proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant. . . . Accordingly, Scarfo's claim that the warrants were written and executed as general warrants is rejected. . . .

The principal mystery surrounding this case was whether the KLS intercepted a wire communication in violation of the wiretap statute by recording keystrokes of e-mail or other communications made over a telephone or cable line while the modem operated. These are the only conceivable wire communications which might emanate from Scarfo's computer and potentially fall under the wiretap statute. . . .

The KLS, which is the exclusive property of the F.B.I., was devised by F.B.I. engineers using previously developed techniques in order to obtain a target's key and key-related information. As part of the investigation into Scarfo's computer, the F.B.I. "did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer." Neither did the F.B.I. "install or operate any KLS component which would search for or record any fixed data stored within the computer."

Recognizing that Scarfo's computer had a modem and thus was capable of transmitting electronic communications via the modem, the F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports. . . . Hence, when the modem was operating, the KLS did not record keystrokes. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated. Since Scarfo's computer possessed no other means of communicating with another computer save for the modem, the KLS did not intercept any wire communications. Accordingly, the Defendants' motion to suppress evidence for violation of Title III is denied. . . .

NOTES & QUESTIONS

1. ***Did the Court Need to Reach the Main Issue?*** Judge Politan discusses the government's actions in *Scarfo* as if a suppression remedy were available for Scarfo. He finds that a search warrant was not required under the Wiretap Act because of the way in which the FBI's keylogging device worked; the KLS did not function when the modem was operating. But there was a simpler way to deny Scarfo's motion: the Wiretap Act does not provide a suppression

remedy for electronic communications. Did Judge Politan assume that a remedy existed according to some theory similar to the *McVeigh* case? Was he simply eager to rule on the KLS issue?

2. ***Recording Thoughts and Ideas.*** Consider the following argument by Raymond Ku:

> . . . By monitoring what an individual enters into her computer as she enters it, the government has the ability to monitor thought itself. Keystroke-recording devices allow the government to record formless thoughts and ideas an individual never intended to share with anyone, never intended to save on the hard drive and never intended to preserve for future reference in any form. The devices also allow the government to record thoughts and ideas the individual may have rejected the moment they were typed. . . .
>
> . . . [T]he techniques used in the Scarfo case bring us closer to a world in which the only privacy we are guaranteed is the privacy found in the confines of our own minds. [78]

3. ***Old Technologies in New Bottles?*** A common defense of new technological surveillance devices is that they are analogous to existing technologies. Carnivore can be likened to pen registers; the keystroke monitor in the Scarfo case can be analogized to a bug. To what extent are these analogies apt? Are new surveillance technologies, simply old forms of surveillance in new bottles? Or is there something different involved? If so, what is new with these technologies, and how ought they be regulated?
4. ***Magic Lantern.*** The FBI has developed technology through which a keystroke logging device can be installed into a person's computer through a computer virus that is e-mailed to the suspect's computer. The virus keeps track of keystrokes and secretly transmits the information to the government. Thus, the government can install a keystroke logging device without ever having to physically enter one's office or home. Recall your Fourth Amendment analysis of Carnivore. How does Magic Lantern differ with respect to its Fourth Amendment implications? How does your Fourth Amendment analysis of Magic Lantern differ from that of the keystroke logging device in *Scarfo*?

[78] Raymond Ku, *Think Twice Before You Type*, 163 N.J. L.J. 747 (Feb. 19, 2001).