ESSAY

DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE

*Orin S. Kerr**

The widespread use of computers in recent years has led to a new type of evidence in criminal cases: digital evidence, consisting of zeros and ones of electricity. In this Essay, Professor Kerr considers whether traditional rules of criminal procedure can effectively regulate investigations involving digital evidence. Kerr concludes that the new methods of gathering digital evidence trigger a need for new legal standards. Existing law is tailored to the gathering of physical evidence and eyewitness testimony; applying that law to digital evidence collection produces a number of surprising results. Professor Kerr contends that new rules are needed, and offers preliminary thoughts on what those rules should look like and which institutions should generate them.

INTRODUCTION

This Essay considers how the law of criminal procedure should change in response to the increasing number of criminal cases based

* Associate Professor, George Washington University Law School. Thanks to John Duffy, Laura Heymann, Mark Lemley, Cynthia Lee, Chip Lupu, Dan Markel, Tom Morgan, Julian Mortenson, Spencer Overton, Steve Schooner, David Sklansky, Daniel Solove, Peter Swire, and Bob Tuttle for their helpful comments on a prior draft.

heavily on digital evidence.[1] It argues that the use of computers in criminal activity has popularized a new form of evidence, digital evidence, and explains how the collection of digital evidence differs from traditional investigative techniques. It contends that the new methods of collecting digital evidence should and must lead to reforms in the law of criminal procedure to regulate digital evidence collection.

Digital evidence should trigger new rules of criminal procedure because computer-related crimes feature new facts that will demand new law. The law of criminal procedure has evolved to regulate the mechanisms common to the investigation of physical crimes, namely the collection of physical evidence and eyewitness testimony. Existing law is naturally tailored to law enforcement needs and privacy threats they raise. Digital evidence is collected in different ways than eyewitness testimony or physical evidence. The new ways of collecting evidence are so different that the rules developed for the old investigations often no longer make sense for the new. Rules that balance privacy and public safety when applied to the facts of physical crime investigations often lead to astonishing results when applied to the methods common in digital evidence investigations. They permit extraordinarily invasive government powers to go unregulated in some contexts, and yet allow phantom privacy threats to shut down legitimate investigations in others.

This Essay contends that the new dynamics demonstrate the need for procedural doctrines designed specifically to regulate digital evidence collection. The rules should impose some new restrictions on police conduct and repeal other limits with an eye to the new facts and new social practices that are common to how we use and misuse computers. Further, we should look beyond the judiciary and the Fourth Amendment for many of these new rules. While some changes can and likely will come from the courts, more can come from legislatures and executive agencies that are able to offer new and creative approaches not tied directly to our constitutional traditions.

Some changes already have begun. A number of new rules are beginning to emerge from Congress and the courts. In the last five years, a few courts have started to interpret the Fourth Amendment differently in computer crime cases. They have quietly rejected traditional rules and substituted new ones. At a legislative level, Congress has enacted computer-specific statutes to address other new threats to privacy. The changes are modest ones so far. Taken together, however, the new constitutional and statutory rules may be seen as the beginning of a new subfield of criminal procedure that regulates the collection of digital evidence.

---

1. Criminal procedure is generally defined as the rules and procedures that the police and prosecutors must follow as they investigate and prosecute criminal activity. See, e.g., Russell Weaver et al., Criminal Procedure: Cases and Materials 2 (2001).

This Essay proceeds in three parts. Part I compares the basic mechanisms of traditional crimes and computer-related crimes. It explains how the switch from physical to electronic crimes brings a switch from physical evidence and eyewitness testimony to digital evidence, and how investigators tend to use very different collection methods for the two types of evidence. Part II turns from the facts to the governing law, focusing on the Fourth Amendment's prohibition on unreasonable searches and seizures. It shows that existing Fourth Amendment doctrine is naturally tailored to the facts of physical crimes, but that a number of difficulties arise when that doctrine is applied to the facts of computer crime investigations. Part III argues that new rules are needed to govern digital evidence collection, and offers preliminary thoughts on what those rules might look like and which institutions should generate them. It also shows that courts and Congress already have begun responding to the problem of digital evidence with a number of computer specific rules.

I. PHYSICAL EVIDENCE VERSUS DIGITAL EVIDENCE

Rules of criminal procedure are organic rules, contingent on the facts of the investigations they regulate. Changing facts exert pressure to change existing legal doctrine. To see why digital evidence creates pressure for new rules of criminal procedure, we need to begin by comparing the investigative facts of traditional crimes to the investigative facts of crimes involving digital evidence. This Part will explore the differences by contrasting two examples. The first example is a traditional bank heist; the second example is a roughly analogous computer crime in which the suspect steals money by hacking into a bank computer. By comparing these two crimes, we can see how the mechanisms of electronic crimes and physical crimes are often distinct. These different mechanisms lead to different evidence, different investigative steps, and, ultimately, the need for different legal rules.

A. *Physical Crimes and Physical Crime Investigations*

Imagine that Fred Felony decides to rob a bank. Fred drives to a local branch office, parks his car outside, and goes in. When it's his turn at the teller, Fred slides over a note that reads, "This is a stick up. Give me all your money and no one will get hurt." The teller sees the note and observes the barrel of a pistol protruding from Fred's jacket. The teller nervously hands Fred a bag of money. Fred grabs the bag and runs out of the bank. Once outside, he jumps into his getaway car and speeds away.

Now imagine that a police detective is called to investigate the bank robbery. His goal is to collect evidence of the crime so that he can identify the robber and then help prove the case in court beyond a reasonable doubt.[2] But how? The detective's first strategy will be to collect eyewit-

2. See In re Winship, 397 U.S. 358, 363–64 (1970) (discussing the reasonable doubt standard).

ness testimony. The detective will ask the teller and other people at the bank to describe what they observed. What did the robber look like? How tall was he? Was his voice unusual? Did anyone see the getaway car? The eyewitness testimony will consist of reports from people about what they observed with their eyes and heard with their ears. By visiting the bank and asking questions, the investigator will become an eyewitness of sorts himself: He will be able to testify about what he saw and heard when he arrived at the bank and investigated the crime.

The detective's second strategy will be to collect physical evidence. Physical evidence will help to connect the crime to a suspect beyond a reasonable doubt. For example, the detective will recover the note that Fred Felony left with the teller and analyze it for fingerprints or distinctive handwriting. Perhaps Fred left behind other physical clues as well. Perhaps he dropped the gun when he rushed out of the bank. Perhaps he lost a button, or dropped a receipt he had been carrying in his pocket. This physical evidence can be presented and explained to the jury to create a powerful tangible connection between the defendant and the crime.[3]

If the eyewitness testimony and physical evidence from the bank do not make the case against Fred, the police may need to look for additional evidence elsewhere. The police may interview other suspects to see if they know who was behind the bank robbery. They may look around town for cars matching the description of the getaway car. If the police have particular suspicions about Fred, they may search his house for evidence such as marked stolen bills or clothes matching those worn by the robber. The goal will be to collect additional eyewitness testimony and physical evidence that can help prove that Fred robbed the bank. If any of these tactics yield additional evidence, the police will add the new evidence to the physical evidence and eyewitness testimony found at the crime scene.

Let's assume the detective gathers sufficient evidence to show that Fred committed the bank robbery. Fred is charged, and the case goes to trial. At trial, prosecutors will assemble the eyewitness testimony and physical evidence to prove that Fred committed the crime. The teller will testify about how Fred Felony approached him and handed him the note. Other eyewitnesses will testify about what they saw and heard during the robbery. Witnesses who are personally familiar with the physical evidence will help shepherd it into evidence so the jury can consider it in the jury room during deliberations.[4] For example, if Fred dropped his gun on the way out of the bank and the detective found it, the detective will take

3. See, e.g., United States v. Patane, 124 S. Ct. 2620, 2631 (2004) (Kennedy, J., concurring) (noting "the important probative value of reliable physical evidence").

4. Evidentiary rules such as Federal Rule of Evidence 901 guide the admission of evidence. Such rules normally require testimony "sufficient to support a finding that the matter in question is what its proponent claims," Fed. R. Evid. 901(a), such as by testimony from a witness with personal knowledge, id. 901(b)(1).

the stand and testify about how and where he found the pistol. The pistol will then be admitted into evidence.[5] If the police executed a search at Fred Felony's home, an agent who participated in the search will testify about what he found. The sequence of witnesses at trial will build the case against Fred Felony and attempt to establish his guilt beyond a reasonable doubt.

B. *Computer Crimes and Computer Crime Investigations*

Now let's switch to an electronic version of this crime. Let's replace the physical visit to the bank and the retrieval of paper money with a virtual "visit" to the bank and the theft of digital funds from a bank computer. The point of the comparison is not to find an exact analog to the physical bank robbery; there are obvious differences between the two.[6] Rather, the goal is to get a sense of how the crime and the evidence changes when we turn from physical crimes to crimes involving digital evidence.

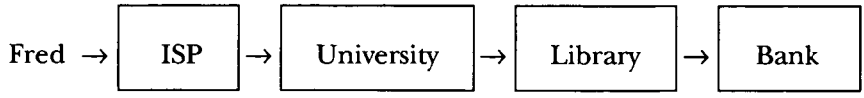
This time, Fred Felony decides to steal money using a computer. Instead of visiting the bank in person, he goes online from his home. Fred logs on to the internet from an account he holds with a local internet service provider (ISP). Although his ultimate goal is to hack into the bank's computers, Fred first loops his attack through a few intermediary computers to disguise his tracks. He picks computers with poor security and little need to keep detailed records of who used their servers. If anyone tries to trace Fred's misconduct back to him, they will have to go through the intermediaries first. Let's say Fred selects a server run by a private university in California as his first intermediary, and a server operated by a public library in Kansas as his second. From his ISP, he first hacks into the university computer; with access to the university computer established, he then hacks into the library computer. With access to the library computer established, Fred targets the bank's main server. After several tries, Fred eventually guesses the master password correctly and

---

5. See, e.g., United States v. Towns, 913 F.2d 434, 439 (7th Cir. 1990) (reviewing physical evidence admitted at trial following a bank robbery, including "a small blue vinyl bag similar to the one that [a] defendant [was carrying during the bank robbery,] an empty ammunition clip that would fit only a .44 caliber magnum semi-automatic pistol" that was recovered from hotel room where defendant stayed on the night of the robbery, as well as "a pair of sunglasses similar to those that defendant Towns allegedly wore during the bank robbery; and . . . several money wrappers that were identical to those that had bound the money that the robbers had taken from the bank").

6. The most obvious difference is that the physical crime involves a threat of physical harm to persons. In the language of criminal law, the physical crime is a robbery; the virtual crime is a form of bank theft. See generally Wayne R. LaFave, Criminal Law 996 (4th ed. 2003) (noting that the crime of robbery "may be thought of as aggravated larceny—misappropriation of property under circumstances involving a danger to the person as well as a danger to property—and thus deserving of a greater punishment than that provided for larceny" (citations omitted)).

logs on to the bank's server. A diagram of the attack might look something like this:



With full system privileges on the bank's computer, Fred sets up a new bank account and instructs the computer that the account contains $500,000. He then wires the money from the new account to an untraceable offshore account. The next day, a bank employee notices that an unauthorized account was created and that money is missing. The bank employee calls the police.[7]

Imagine the case is assigned to the same detective who investigated the physical bank robbery. Once again, his goal is to gather enough evidence to identify the wrongdoer and establish a case in court. But how? The detective will immediately notice that the crime scene looks very different. There are no eyewitnesses at the bank, and there is no physical evidence. No one saw the intrusion occur, and there is no tangible evidence to manipulate. From the standpoint of the human senses, the crime occurred inside closed wires and boxes via the rapid shifting of invisible and silent electrical impulses. Computer technicians and system administrators can look through computer files and try to reconstruct what happened. They can observe what their computer screens show them. But the underlying evidence is no longer eyewitness testimony or physical evidence. It is digital evidence: zeros and ones of electricity.

How to begin the investigation? The detective's first step will be to ask the system administrator in charge of the bank's computer to gather all of the information relating to the theft that may be stored on the computer. In all likelihood, this information will tell him very little. With the physical crime, the chances were good that the crime scene would yield substantial leads. Even if no one could identify Fred in a lineup, his physical presence at the crime scene greatly narrowed the number of suspects. The electronic crime scene looks very different. In most cases, evidence gathered at the victim site will tell the investigator only that someone, located somewhere in the world, hacked into the bank. In most cases, the biggest investigative lead comes in the form of an originating Internet Protocol (IP) address recorded by the bank's servers. An IP address is the internet equivalent of a telephone number;[8] the bank's server likely kept a log of Fred's connection to the bank computer and

7. This hypothetical is loosely based on a case from 1995. A computer hacker named Vladimir Levin, located in St. Petersburg, Russia, hacked into Citibank computers, set up various accounts, filled them with money, and then had coconspirators withdraw the money. See, e.g., William M. Carley & Timothy L. O'Brien, How Citicorp System Was Raided and Funds Moved Around World, Wall St. J., Sept. 12, 1995, at A1.

8. See generally Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 407 n.4 (2d Cir. 2004) (posthumously published draft opinion of Parker, C.J.) (defining an Internet Protocol address as "[t]he unique identification of the location of an end-user's computer [which]

recorded its originating IP address as part of that log. To find Fred Felony, the detective must start with the IP address and try to follow the trail of electronic bread crumbs from the bank back to Fred's home computer.[9] He must find and collect the bits and bytes of digital evidence stored around the country (if not around the world), and assemble them in a way that identifies Fred and establishes his guilt beyond a reasonable doubt.

The process of collecting electronic evidence in computer hacking cases generally divides into three steps. It begins with the collection of stored evidence from third-party servers, turns next to prospective surveillance, and ends with the forensic investigation of the suspect's computer. These three steps encompass the basic mechanisms of digital evidence collection: collecting digital evidence while in transit, collecting digital evidence stored with friendly third parties, and collecting digital evidence stored with hostile parties such as the target. Each mechanism presents unique facts and requires special considerations.

The first and most basic investigative step is obtaining stored records from the system administrators of the various computer servers used in the attack. Fred connected to four computers to commit his offense: servers operated by his ISP, the university, the library, and the bank. It is possible (although not certain) that each of these servers retained records of Fred's connection. The detective will attempt to assemble these records to trace back the attack from the bank's server through the intermediary computers to the ISP in a step-by-step fashion. This cumbersome procedure is necessary because the packets that carry internet communications list only their immediate origin and destination points.[10] If Fred launches an attack from his ISP through the university and library servers and then onto the victim bank, the communications received at the bank computer will bear the originating IP address of the library server, not Fred's ISP. The detective must contact the system administrator at the library to determine if they have any records of the connection to the bank at the particular time that the attack occurred. If comprehensive records exist at the library, those records should indicate that the attack against the bank originated at the university. The detec-

---

serves as a routing address for email and other data sent to that computer over the Internet from other end-users").

9. Cf. Michael L. Rustad, Private Enforcement of Cyhercrime on the Electronic Frontier, 11 S. Cal. Interdisc. L.J. 63, 98 (2001) (noting that for investigators of internet crimes there are no geographical borders and thus there is no "traditional crime scene").

10. Orin S. Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 663 (2003) [hereinafter Kerr, Internet Surveillance]. This is true because the internet is a packet-switched network, and a communication intentionally sent from A to B to C is normally routed via two different stages of packets: First, a packet is made to send the information from A to B, then at B a new packet is created to send the communication from B to C. As a consequence of this architecture, the packet only indicates the source of the most recent packetizing. See id. at 663 n.284.

tive will then repeat the process by contacting the system administrator at the university. If comprehensive records exist at the university, those records will indicate that the attack originated not at the university, but at Fred's ISP. The detective will then contact Fred's ISP. If comprehensive records exist at the ISP, those records should indicate that Fred's account was being used to access the internet at the time of the attack. The ISP should also have a credit card or billing address for Fred in its records, allowing the detective to focus the investigation on Fred.[11]

Investigations are rarely this simple, however. The trail of evidence usually is interrupted somewhere along the way. Few system administrators keep comprehensive records, and those records that are kept often are deleted after a brief period of time.[12] Hackers routinely target intermediary computers known to keep few or no records so as to frustrate investigators. When the chain of stored records contains a broken link, the detective must shift gears to a second method of evidence collection I have elsewhere called prospective surveillance.[13] Prospective surveillance refers to the use of logging software or hardware to monitor future internet traffic and create a record of that traffic. The scope of prospective surveillance depends on where the surveillance device is installed and how it is configured. It may encompass invasive wiretapping that intercepts private e-mails, or may merely point to the most immediate source address of an attack.

The basic idea behind prospective surveillance is that criminal activity may reoccur or be ongoing, and investigators and victim system ad-

---

11. For example, in United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000), FBI investigators determined that a computer assigned the IP address 24.94.200.54 contained illegal images of child pornography. Investigators contacted Road Runner, the ISP that controlled this IP address, and obtained the following information:

> The subscriber whose computer used I.P. address 24.94.200.54 on July 2, 1999, at 11:49 p.m. was Rosemay (sic) D. Kennedy of 9120 Harvest Court, Wichita, Kansas, telephone 316-722-6593. Two users were listed for that account: RKENNEDY@KSCable.COM and KENNEDYM@KSCable.Com. The account had been active since June 7, 1999.

Id. at 1107.

12. See Computer Crime and Intellectual Prop. Section, U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 104–07 (2002), available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (on file with the *Columbia Law Review*) [hereinafter DOJ Manual]. The manual notes that:

> Some providers retain records for months, others for hours, and others not at all. As a practical matter, this means that evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, agents may learn of a child pornography case on Day 1, begin work on a search warrant on Day 2, obtain the warrant on Day 5, and then learn that the network service provider deleted the records in the ordinary course of business on Day 3.

Id. at 104–05.

13. See Kerr, Internet Surveillance, supra note 10, at 616–18 (explaining distinction between prospective and retrospective surveillance).

ministrators can complete the missing links in the chain of evidence by monitoring future activity. Fred may come back to try to set up another account and siphon away more money. If the evidence trail went cold at the bank server itself, the bank can monitor its server for unauthorized efforts to set up an account. If the trail went cold at the university, the police may install a monitoring device at the university server to monitor any communications directed from the server to the bank. If Fred Felony strikes again, prospective surveillance can create a fresh trail of evidence back to Fred's ISP.[14]

This brings us to the third and final stage of electronic evidence collection. Recall that in the case of Fred's physical crime, it was possible that the police would need to execute a search warrant at his home to gather sufficient proof that Fred committed the robbery. In the digital version of the crime, that step is likely to be essential. Digital evidence taken from servers may show that a particular account was used to steal money from the bank, but will almost never prove that a particular person was controlling the account.[15] Something important is missing: A substitute for biometric eyewitness testimony or physical evidence to connect the existing evidence to a specific person. Without that connection, the government will be unable to prove their case beyond a reasonable doubt.

The key in most cases will be recovering the computer used to launch the attack. If the police can find and analyze Fred's home computer, it will likely yield damning evidence. The records kept by most operating systems can allow forensics experts to reconstruct with surprising detail who did what and when.[16] Even deleted files often can be recovered,[17] as a delete function normally just marks storage space as available for new material and does not actually erase anything.[18] An analysis of the computer may reveal a file containing the bank password used to set up the unauthorized account.[19] It may reveal records from that account, or records taken from some of the intermediary computers. Even if no such documents are found, it may be possible to tell whether the attack was launched from the computer. Such proof can provide persua-

14. One early example of how such a trail of evidence might be traced back to a suspect is recounted in Cliff Stoll's *The Cuckoo's Egg*. See Cliff Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (1990).

15. As the Justice Department has recognized, "generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it." See DOJ Manual, supra note 12, at 69.

16. See Eric Friedberg, Catch as Cache Can: Forging or Altering Electronic Documents Leaves Tell-Tale Fingerprints Behind, Legal Times, Feb. 2, 2004, at 36.

17. See, e.g., United States v. Upham, 168 F.3d 532, 533 (1st Cir. 1999).

18. See James M. Rosenbaum, In Defense of the Delete Key, 3 Green Bag 2d 393, 393 (2000).

19. See, e.g., United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997). In *Whitaker*, the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included a spreadsheet file detailing records of narcotics sales and amounts owed to him by his coconspirators. See id.

sive evidence of guilt. While innocent explanations may exist for why the suspect's personal computer was used to launch an attack, connecting the attack to the suspect's private property can go a long way toward eliminating reasonable doubt.

Computer forensics experts have developed a detailed set of procedures that forensic analysts ordinarily follow when they seize and analyze a target's computer.[20] The technical details aren't important here, but the broad outline is. First, the detectives ordinarily seize the computer and bring it back to a government forensic laboratory for analysis.[21] This is considered necessary because the forensic process is very time consuming; computer experts normally cannot find the evidence on a hard drive in the time that would allow the search to occur on site.[22] Back at the lab, the analyst begins by generating a "bitstream" or "mirror" image of the hard drive.[23] The bitstream copy is an exact duplicate, not just of the files, but of every single bit and byte stored on the drive.[24] The analyst then performs his work on the copy rather than the original to ensure that the original will not be damaged or altered by the analyst's investigation.[25]

The analyst may try a range of techniques to locate the evidence sought. For example, the examiner may begin by executing string searches for particular extensions, phrases, or textual fragments that relate to the evidence justifying the search. Alternatively, he may open all files with particular characteristics or sample from the files until he finds the evidence linking the suspect to the crime. In Fred's case, for exam-

---

20. See generally Bill Nelson et al., Guide to Computer Forensics and Investigations (2004) (surveying current computer forensics practices).

21. See DOJ Manual, supra note 12, at 44 ("As a practical matter, circumstances will often require investigators to seize equipment and search its contents off-site.").

22. See United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant.").

23. As the Justice Department has explained:

> Creating a duplicate copy of an entire drive (often known simply as "imaging") is different from making an electronic copy of individual files. When a computer file is saved to a storage disk, it is saved in randomly scattered sectors on the disk rather than in contiguous, consolidated blocks; when the file is retrieved, the scattered pieces are reassembled from the disk in the computer's memory and presented as a single file. Imaging the disk copies the entire disk exactly as it is, including all the scattered pieces of various files (as well as other data such as deleted file fragments). The image allows a computer technician to recreate (or "mount") the entire storage disk and have an exact copy just like the original. In contrast, a file-by-file copy (also known as a "logical file copy") merely creates a copy of an individual file by reassembling and then copying the scattered sectors of data associated with the particular file.

DOJ Manual, supra note 12, at 42 n.6.

24. See id.

25. See, e.g., United States v. Triumph Capital Group, 211 F.R.D. 31, 48 (D. Conn. 2002).

ple, an investigator might begin by searching the hard drive for the bank's password, or perhaps for the name of the bank. If that doesn't work, the investigator might begin looking for documents date stamped on the day of Fred's attack, or might just look for any financial documents. Once he understands how Fred stored the data on his hard drive, the investigator may find a great deal of incriminating information. Assuming Fred was not tipped off to the investigation and has not permanently erased the relevant files, the analyst may find the bank's master password, account records, and other evidence linking the computer and its owner to the crime.

Let's assume that these tactics are successful, and that an analysis of Fred's computer reveals evidence of the attack. Fred is charged, and the case goes to trial. The prosecutor will put witnesses on the stand in a way that tracks the course of the investigation. First, a bank employee will testify about the attack and the bank's losses. Next, the system administrators of the intermediary computers will testify about their link in the chain of evidence, and an employee from Fred's ISP will testify about the electronic clues leading back to Fred's account. Finally, government agents will testify. The detective will testify that he recovered the computer inside Fred's home, and the computer forensics expert will testify that Fred's computer contained evidence of the attack together with Fred's personal files. The government's case now proves beyond a reasonable doubt that Fred committed the online bank theft.

II. Digital Evidence and the Failure of Existing Rules

Existing rules of criminal procedure are organic products naturally tailored to the facts of physical crime investigations. Comparing the contours of existing rules of criminal procedure to the investigative steps common to such traditional investigations reveals an obvious match. The contemporary rules of criminal procedure are physical-world rules that reflect the realities of physical-world investigations. They attempt to balance privacy and law enforcement needs in light of the facts of how police collect physical evidence and eyewitness testimony.[26]

Applying existing doctrine to the collection of digital evidence produces some startling results, however. Rules that sensibly regulate the investigation of physical crimes based on physical facts lead to surprising outcomes when applied to the new investigations. At many stages, those outcomes impose few if any limits on government investigations. At a few stages, they impose unnecessary barriers to successful investigations. This Part demonstrates how existing rules work reasonably well in traditional cases, but often fail to regulate the collection of digital evidence effectively.

---

26. C.f. Nadine Strossen, The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis, 63 N.Y.U. L. Rev. 1173, 1181–84 (1988) (describing the use of balancing tests in Fourth Amendment law).

A. *Physical Crimes and Rules of Criminal Procedure*

Existing rules of criminal procedure are naturally tailored to the facts of physical-world crimes. Consider the Fourth Amendment's prohibition on unreasonable searches and seizures.[27] The Fourth Amendment's rules on unreasonable "searches" regulate the collection of evidence in the form of eyewitness testimony by police officers. The search rules govern where and in what circumstances officers can go to report what their senses observe.[28] By regulating where officers can go, the search rules regulate what officers see and hear; by regulating what they see and hear, the rules limit the scope of evidence they can collect. This function is often obscured by the Court's famous quip in *Katz v. United States* that "the Fourth Amendment protects people, not places."[29] As Justice Harlan noted in his *Katz* concurrence, the question of what protection it provides to people "requires reference to a 'place.'"[30] Under Justice Harlan's formulation, the Fourth Amendment remains heavily tied to places; in William Stuntz's formulation, the law "regulate[s] what police officers can see and hear," focusing on where they can go more than what they do once they get there.[31]

Specifically, the *Katz* "reasonable expectation of privacy" test has been interpreted in a way that effectively demarcates physical spaces that are public from physical spaces that are more private.[32] An officer can enter any space that is not protected by a reasonable expectation of privacy; such an entrance does not count as a "search."[33] This allows officers to roam public streets or other places open to the public without restriction. In contrast, an officer can enter spaces protected by a reasonable expectation of privacy only under special circumstances. The entry into private space such as a home or an office constitutes a search, and is reasonable (and therefore constitutional) only if justified by special circumstances.[34] Those special circumstances might include the presence of a valid search warrant, the consent of someone with common authority

27. U.S. Const. amend. IV.

28. See William J. Stuntz, Reply, 93 Mich. L. Rev. 1102, 1102–03 (1995) [hereinafter Stuntz, Reply] (noting that "[t]he Fourth Amendment regulates street stops, but it pays little attention to how coercively the police behave in those stops—instead, the law concerns itself with whether and when the police can look in suspects' pockets").

29. 389 U.S. 347, 351 (1967).

30. Id. at 361 (Harlan, J., concurring).

31. Stuntz, Reply, supra note 28, at 1102. Stuntz goes on to note that "the law limits police officers' ability to enter people's houses but turns a blind eye to how violently the cops behave once inside." Id. at 1103.

32. For a discussion of how the "reasonable expectation of privacy" test applies to investigative steps involving technologies that can conduct searches without invading physical space, see Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 827–837 (2004) [hereinafter Kerr, New Technologies].

33. Illinois v. Andreas, 463 U.S. 765, 771 (1983).

34. Smith v. Maryland, 442 U.S. 735, 739–40 (1979).

over the space, or the existence of exigent circumstances.[35] Once an investigator has legitimately entered a particular space, he is free to testify about whatever he observes without implicating the Fourth Amendment.[36] The police need not "avert their eyes from evidence of criminal activity."[37] Anything the officer sees is in "plain view,"[38] anything he smells is in plain smell,[39] and anything he overhears is not protected under the Fourth Amendment.[40]

While the search rules regulate the collection of eyewitness testimony by police officers, the seizure rules govern the collection of physical evidence. The Supreme Court has defined a "seizure" of property as "meaningful interference with an individual's possessory interests in that property."[41] Under this test, the gathering of physical evidence is a seizure. Fourth Amendment cases explain when such seizures are reasonable, and thus allowable. Very brief seizures undertaken for legitimate law enforcement purposes are usually reasonable,[42] but extended seizures are usually unreasonable unless the police obtain a warrant.[43] Seizures that do not infringe directly on possessory interests are usually reasonable; for example, an investigator can take evidence if its owner consents,[44] or if the evidence has been abandoned.[45]

Constitutional provisions beyond the Fourth Amendment also regulate traditional investigative steps. The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself."[46] This right against self-incrimination limits the collection of eyewitness testimony by regulating when investigators can use statements against a defendant. Similarly, the Sixth Amendment guarantees every

---

35. Illinois v. Rodriguez, 497 U.S. 177, 183–84 (1990).

36. But see Harold J. Krent, Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment, 74 Tex. L. Rev. 49, 51 (1995) (arguing that Fourth Amendment should be interpreted to provide use restrictions on information gathered by government).

37. California v. Greenwood, 486 U.S. 35, 41 (1988).

38. Horton v. California, 496 U.S. 128, 135 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 465–66 (1971) (Stewart, J., concurring)).

39. United States v. McCoy, 200 F.3d 582, 584 (8th Cir. 2000).

40. Hoffa v. United States, 385 U.S. 293, 302 (1966). This is true even if a suspect may reasonably suspect that the person may not understand what he is overhearing. See United States v. Longoria, 177 F.3d 1179, 1183–84 (10th Cir. 1999).

41. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

42. See Illinois v. McArthur, 531 U.S. 326, 330 (2001) ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.").

43. United States v. Place, 462 U.S. 696, 701 (1983) (noting that in "the ordinary case," seizures of personal property are "unreasonable within the meaning of the Fourth Amendment unless . . . accomplished pursuant to a judicial warrant," issued after finding probable cause).

44. Schneckloth v. Bustamonte, 412 U.S. 218, 219–20 (1973).

45. Abel v. United States, 362 U.S. 217, 241 (1960) (holding that it is lawful for government investigators to seize abandoned property).

46. U.S. Const. amend. V.

defendant "compulsory process for obtaining witnesses in his favor,"[47] empowering defendants to collect eyewitness testimony of their own. Both sets of rules are focused on balancing the rights of the government and the defendant in traditional investigations into traditional crimes.

We can see how traditional rules of criminal procedure work in practice by revisiting the investigation into Fred's physical bank robbery. The detective is free to examine the outside of the bank: There is no reasonable expectation of privacy in that which is exposed to the public.[48] He can enter the bank during business hours to look around, as well; because the bank is open to the public, entering the bank is not a search. If he wants to look more closely at the bank after hours, however, he needs the consent of a bank employee. Consent will render the search reasonable, and therefore constitutionally permissible. The investigator can also speak with eyewitnesses and record their observations of the crime. If the investigator finds Fred Felony's gun, he can seize it: The seizure is reasonable under the Fourth Amendment so long as the gun's usefulness as evidence is immediately apparent.[49] If he comes across other evidence with no apparent relation to the crime, however, he normally cannot seize it. If the police opt to search Fred's house for evidence, they will need a search warrant to justify the entry into his private space.[50] The Fourth Amendment rules governing search warrants ensure that the search will be narrowly tailored: It must be limited to the particular physical place where the evidence is likely present and the search must be limited to specific items associated with the bank robbery.[51] The detective is then free to testify about whatever he observed during the investigation. Taken together, the existing rules of criminal procedure effectively regulate the collection of physical evidence and eyewitness testimony.

B. *Digital Evidence and Physical-World Rules*

The picture changes considerably when we switch from traditional investigations involving eyewitness testimony and physical evidence to investigations requiring the collection of digital evidence. As noted earlier, there are three basic mechanisms of digital evidence collection: the collection of stored evidence from third parties, the collection of stored evidence from the target, and the collection of evidence in transit. Applying existing doctrines to these three mechanisms reveals several difficulties.

---

47. Id. amend. VI.

48. See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (noting that what is exposed to the public cannot receive Fourth Amendment protection).

49. Horton v. California, 496 U.S. 128, 136 (1990) (citing Coolidge v. New Hampshire, 403 U.S. 443, 466 (Stewart, J., concurring) (1971)).

50. Kyllo v. United States, 533 U.S. 27, 40 (2001).

51. See, e.g., *Horton*, 496 U.S. at 138–40; United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982) (noting that probable cause to seize specific paper files enumerated in warrant does not permit seizure of commingled innocent files).

The traditional rules tend not to translate well to the new facts. Caution is warranted: Surprisingly few cases exist that apply traditional doctrine to the collection of digital evidence. Mapping the old rules onto the new facts requires some speculation. At the same time, a comparison of the basic contours of existing law and the dynamics common to digital evidence cases demonstrates the poor fit between them. In many circumstances, the traditional rules fail to provide any real limit on law enforcement practices. In other circumstances, they allow phantom privacy threats to block necessary investigative steps.

1. *Evidence from Third Parties and the Subpoena Process.* — Consider the first stage of most electronic crime investigations, in which investigators contact system administrators and obtain stored evidence relating to the crime from servers used in the course of the crime.[52] This process raises important privacy concerns suggesting the need for careful legal regulation. Internet users routinely store most if not all of their private information on remote servers, and all of that information is available to system administrators.[53] System administrators can read private e-mail, look through stored files, and access account logs that record how individual subscribers used the network. As a result, the power to compel evidence from ISPs can be the power to compel the disclosure of a user's entire online world. Plus, disclosure can occur without notice to the user, and it can involve multiple accounts. The power to compel evidence from ISPs can be the power to disclose the online profile of hundreds or even thousands of users at once, all in total secrecy.

Remarkably, existing Fourth and Fifth Amendment doctrine offers virtually no privacy protection to regulate this process. Investigators can compel system administrators to disclose information stored on their servers using subpoenas.[54] Subpoenas are lightly regulated by the Fourth Amendment: Existing law requires only that the information or property to be compelled must be relevant to an investigation, and that its production must not be overly burdensome to the recipient of the subpoena.[55] The relevance standard covers almost everything, as it includes merely checking to make sure that no crime has been committed.[56] The limits

52. See supra notes 8–11 and accompanying text.

53. See, e.g., Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1092–94 (2002) (discussing information stored by service providers).

54. The two most common types of subpoenas track the traditional evidence gathering techniques in physical-world crimes. They are subpoenas ad testificandum, subpoenas to testify before a grand jury, and subpoenas duces tecum, subpoenas ordering the recipient to give physical evidence to the grand jury. See Black's Law Dictionary 1467 (8th ed. 2004).

55. See United States v. Dionisio, 410 U.S. 1, 10 (1973) (noting that forcing compliance with a grand jury subpoena raises minimal privacy concerns).

56. See United States v. Morton Salt Co., 338 U.S. 632, 642–43 (1950) (noting that a grand jury subpoena can be issued even just to make sure that no crime has been committed).

of burdensomeness are similarly toothless in the context of electronic evidence: It is generally simple for an ISP to copy voluminous files and give the copy to investigators.[57] Indeed, there can be an inverse relationship between the amount of evidence investigators seek and the burden it places on the recipient of the subpoena; ISPs often find it easier to hand over information en masse rather than filter painstakingly through files to identify the precise file sought.[58] The person under investigation need not be informed of the subpoena's existence.[59] No Fifth Amendment privilege applies because the recipient of the subpoena is an innocent third party.[60] In light of these realities, applying the traditional Fourth and Fifth Amendment rules to the new network crimes leaves the first stage of network crime investigations almost entirely unregulated.

How could the law allow such an astonishing result? The explanation lies in the shift from the role that third-party evidence collection plays in traditional investigations to the role it plays in digital evidence cases. In the past, third-party evidence collection has played a narrow but important role that implicates privacy in relatively limited ways. The role is narrow because perpetrators of physical crimes generally keep the evidence to themselves rather than give it to third parties. If Fred Felony robs a bank, he is going to keep the loot and store his tools in a secure location. He is not likely to share incriminating evidence with people he doesn't know. In that context, the subpoena power poses a relatively small threat of invasive government overreaching. If a police officer suspects that Fred Felony is the bank robber, he cannot simply issue a subpoena ordering Fred to hand over any evidence or fruits of the crime. As a practical matter, Fred would be unlikely to comply, and issuance of the subpoena would tip him off to the investigation. As a legal matter, Fred would enjoy a Fifth Amendment privilege to decline compliance with the subpoena. Because complying would show knowledge and possession of the loot, the privilege against self-incrimination would render the subpoena a legal nullity.[61]

---

57. Cf. William J. Stuntz, Commentary, O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment, 114 Harv. L. Rev. 842, 857–58 (2001) [hereinafter Stuntz, Commentary] ("[W]hile searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.").

58. In my experience working with ISPs in digital evidence investigations, system administrators occasionally expressed willingness to turn over many gigabytes of information relating to thousands of customers rather than go through the trouble of searching through their files for the documents relating to the target of the investigation.

59. See SEC v. O'Brien, Inc., 467 U.S. 735, 743 (1984) (rejecting arguments that a suspect is entitled to notice of a third-party administrative subpoena).

60. See Fisher v. United States, 425 U.S. 391, 397 (1976) (holding that Fifth Amendment privilege does not immunize third-party agent from complying with subpoena directed to suspect's information in the agent's possession).

61. United States v. Hubbell, 530 U.S. 27, 36–37 (2000). Even beyond these practical concerns, there are the very different ways in which subpoenas and direct searches

Subpoenas do serve an important purpose in a specific set of traditional cases: They are essential in document-intensive white-collar crime investigations. As William Stuntz has observed, the weak protections that regulate the subpoena power can be understood at least in part as a contingent product of Fourth Amendment history.[62] In the early case of *Boyd v. United States*, the Supreme Court took the view that an order to compel the disclosure of evidence should be regulated just as carefully as a direct search involving the police knocking down your door.[63] The Court backed off that standard twenty years later in *Hale v. Henkel*, however, when it replaced *Boyd* with the low threshold that a subpoena satisfied the Fourth Amendment so long as it was not "sweeping."[64] Today the law remains roughly similar to that announced a century ago in *Henkel*.[65] Why the change? The regulatory climate of the late nineteenth and early twentieth centuries had seen the rise of white-collar crime investigations, and those investigations demanded easy access to documents that could prove wrongdoing.[66] As Stuntz has explained, "a probable cause standard for subpoenas would end many white-collar criminal investigations before they had begun."[67] The combination of the essential role for subpoenas in a narrow class of document-intensive cases and the generally limited threat to privacy elsewhere has combined to create an environment in which the subpoena process is only very lightly regulated.

A lax subpoena rule makes no sense for computer-network crime investigations, however. Computer users often store much of their informa-

---

pursuant to warrants are executed. Consider Judge Henry Friendly's rationale for why the Fourth Amendment offers little regulation of subpoenas. He looked to the physical mechanism of how the orders are executed:

> The [direct search] is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court.

United States v. Doe, 457 F.2d 895, 898 (2d Cir. 1972).

62. See Stuntz, Commentary, supra note 57, at 857–59.

63. 116 U.S. 616, 630 (1886). *Boyd* involved an order to disclose customs invoices. The Court suggested that there was no Fourth Amendment difference between a direct search and an order to disclose:

> Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of [the Fourth Amendment].

Id.

64. 201 U.S. 43, 76 (1906).

65. See United States v. Dionisio, 410 U.S. 1, 11 (1973) (affirming the rule of *Hale*).

66. See Stuntz, Commentary, supra note 57, at 859.

67. Id. at 860. Stuntz continues: "In short, if the government is to regulate business and political affairs—the usual stuff of white-collar criminal law—it must have the power to subpoena witnesses and documents before it knows whether those witnesses and documents will yield incriminating evidence." Id.

tion with third-party servers. It's how the internet works. Applying the traditional rule to the new facts suggests that the entire internet world of stored internet communications can be subpoenaed via the intermediaries of ISPs. Neither the Fourth Amendment nor the Fifth Amendment offers much protection. The Fourth Amendment does little because its privacy rules are so weak, and the Fifth Amendment fails because third parties such as ISPs can divulge information without implicating any privilege against self-incrimination of their own.[68] Whereas the subpoena power is fairly narrow in traditional cases, in computer crime cases it is incredibly broad. For investigators, compelling the ISP to disclose information is even preferable to the alternative of searching through the ISP's server directly: Officers can simply fax a copy of the subpoena to the ISP's headquarters and await a package or return fax with the relevant documents.[69] No technical expertise or travel to the ISP is required. A reasonable rule developed in response to the realities of physical-world investigations turns into an unreasonable and unbalanced rule when applied to the new facts of digital crime investigations.

2. *Prospective Surveillance and the Problem of Wiretapping.* — We encounter similar problems when investigators conduct prospective surveillance by monitoring a stream of internet traffic.[70] Prospective surveillance can be broad or narrow, depending on what information the investigators seek. The basic investigative step is the same in every case, however: The only difference between broad and narrow surveillance lies in how the filter is configured. This is true because the internet works by jumbling information together during transmission, and tasking computers that receive the information to reassemble it.[71] The zeros and ones passing through a particular cable at a particular time could be anything—part of a very private message, the front page of NYTimes.com, an image of pornography, a hacker's command to a remote server, or generally meaningless computer-to-computer network traffic. The filter setting determines the information collected, with an open setting resulting in total surveillance and an advanced setting tightly regulating the type and amount of information collected.

Although no court has applied the Fourth Amendment to these precise facts, existing doctrine appears poorly equipped to regulate prospec-

---

68. Fisher v. United States, 425 U.S. 391, 398–99 (1976) (holding that the Fifth Amendment does not regulate a subpoena served on tax preparer for tax documents given to the preparer by customers).

69. United States v. Bach, 310 F.3d 1063, 1067–68 (8th Cir. 2002) (holding that such a procedure pursuant to a warrant does not violate the Fourth Amendment).

70. Prospective surveillance can occur in the context of any computer network, and is not limited to cases involving the internet and internet packets. For the sake of simplicity, however, I will focus on the case of prospective surveillance involving packetized internet traffic.

71. See Vincenzo Medillo et al., A Guide to TCP/IP Internetworking (1996), at http://www.ictp.trieste.it/~radionet/nuc1996/ref/tcpip/part1.htm (on file with the *Columbia Law Review*) (describing the internet as transmitting separate packets of data).

tive surveillance. From the standpoint of policy, a sensible rule might permit police officers to collect information that tends to be less private under relatively relaxed rules, but require greater authority such as a search warrant to authorize collection of more private information. The legal threshold would hinge on the filter setting, linking the degree of privacy protection to the invasiveness of the monitoring. If detectives merely want to determine the originating IP address of a particular communication, a low threshold should be imposed; if detectives wish to monitor private e-mails, the law should impose a high threshold.

Generating such a rule from Fourth Amendment doctrine proves surprisingly difficult. The first problem is that Fourth Amendment rules traditionally focus on the justification for entry into a space, not whether the item to be seized after the space is entered should be deemed public or private. The police need a warrant to enter your home regardless of whether they plan to read your personal diary or just want to see the morning newspaper and break in to read your copy.[72] Similarly, the police do not need a warrant to collect and analyze your private documents left out in a public park.[73] The traditional focus on the entry into the space makes sense for physical investigations. In the physical world, regulation of where an officer goes determines what the officer will see, smell, hear, and feel. The officer's human senses will record observations that the officer can later recall and testify about in court. Regulating entry therefore serves as a functional way of regulating evidence collection.[74] The "reasonable expectation of privacy" test divides public from private, limiting observation to public spaces absent special reasons justifying entrance into private spaces.

This focus makes little sense when applied to prospective surveillance. The entry to the tapped line of internet traffic occurs regardless of whether the monitoring is extremely narrow or breathtakingly broad. Instead of representing a crossing of the line between public and private, entry is now merely a prerequisite for any evidence collection. It is presently unclear whether or when internet users have a reasonable expecta-

72. See Soldal v. Cook County, 506 U.S. 56, 69 (1992) ("[T]he reason why an officer might enter a house or effectuate a seizure is wholly irrelevant to the threshold question whether the Amendment applies. What matters is the intrusion on the people's security from governmental interference."); cf. Arizona v. Hicks, 480 U.S. 321, 325 (1987) ("It matters not that the search uncovered nothing of any great personal value to respondent . . . . A search is a search, even if it happens to disclose nothing [of importance].").

73. See United States v. Procopio, 88 F.3d 21, 26–27 (1st Cir. 1996) (holding that, for purposes of the Fourth Amendment, it was not "unreasonable" for police to search papers left openly available in public park).

74. Of course, once a space has been entered, there may be additional subspaces within that space the entry into which can be regulated separately by the Fourth Amendment. See United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978) (holding that officer's entrance into suspect's room was justified by suspect's mother's consent, but that the mother's consent did not justify officer's opening of locked footlocker located in the room).

tion of privacy in their internet communications, and thus whether a wire containing internet traffic should be deemed private or public space for Fourth Amendment purposes.[75] As I have explained elsewhere, significant arguments exist for both positions.[76] But either way, the resulting legal rule would no longer correlate with the invasiveness of the relevant surveillance practice. If courts view wires of internet traffic as public spaces in which individuals cannot retain a reasonable expectation of privacy, traditional rules will impose no constitutional limits on prospective surveillance. If courts construe them as private spaces that do support a reasonable expectation of privacy, surveillance designed to target even nonprivate information will nonetheless require strong legal justification.[77] Neither rule matches intuitive notions of how the law should divide public from private.

The basic problem remains even if courts move beyond this difficulty and try to protect private material more directly. Imagine that courts hinge the scope of Fourth Amendment protections on whether the particular information collected seems public or more private. While this sounds plausible in theory, it proves quite difficult to attain in practice. Technology provides the first hurdle. Existing surveillance filters can identify types of traffic, such as the difference between an e-mail and a web page. Filters can identify particular words, or record communications from or to particular internet addresses. But no filter can make an informed judgment as to whether a particular set of zeros and ones is public or private. The difficulty is not just the technology, but the limits of deduction: Communications normally will not indicate who or what sent or received them, or the context in which they were sent or received. Without that information, it is hard to tell whether particular zeros and ones happen to be part of a communication that the Fourth Amendment might protect in an analogous physical setting. The architecture of the physical world solves this problem in traditional cases by demarcating public spaces from private ones. The same goes for traditional wiretapping over phone lines. When tapping a phone line necessarily intercepts a human-to-human call, the phone line is akin to a virtual private

---

75. See Kerr, Internet Surveillance, supra note 10, at 629 (noting possibility that courts may not find Fourth Amendment protection for internet communications).

76. See Amicus Curiae Brief of Professor Orin Kerr in Support of the Appellant at 6–8, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), available at 2002 WL 32139374 (explaining that courts may view information transmitted across the internet either as equivalent of stored postal mail, in which case it is entitled to Fourth Amendment protection, or as equivalent of information disclosed to a third party, in which case it is not).

77. Cf. Berger v. New York, 388 U.S. 41, 58–60 (1967) (applying the Fourth Amendment to a wire communication in context of a wiretap). *Berger* addressed a facial challenge to a state wiretap statute, making it difficult to apply its principles to an as-applied factual context. At the same time, *Berger* does suggest that the act of wiretapping rather than the precise information collected is the core constitutional concern.

booth.[78] Everything on the line is private. In the case of prospective surveillance of internet communications, however, private and public are mixed together. There is no obvious way to obtain the context needed to draw traditional Fourth Amendment lines.

3. *Searching the Target's Computer and the Warrant Rules.* — The final stage of computer crime investigations exposes particularly deep problems of fit between traditional rules and the new facts. At this stage, the police seize and then analyze the suspect's personal computer. A warrant is plainly required, both to enter the home and to seize the suspect's property.[79] But how much does the warrant actually limit what the police can do? In traditional cases, the rules governing the warrant process ensure that the search and seizure remain relatively narrow. The warrant must name both the specific place to be searched and the specific evidence to be seized.[80] The seizure must be limited to the evidence described in the warrant—which itself is limited by the scope of probable cause to believe that the evidence is on the premises—as well as other evidence discovered in plain view during the course of the search.[81] These rules help ensure that warrant searches do not devolve into general warrants that authorize general rummaging through a suspect's property.[82]

Applying these rules to digital evidence sets up a series of puzzles, however. Consider the first step of the seizure process, in which investigators take the defendant's computer off-site for forensic testing. Seizure of the entire computer is necessary for practical reasons, but can be difficult to justify based on the traditional rules. In many cases, computer hardware is merely a storage device for evidence rather than evidence itself. The evidence is the electronic file that the police are looking for and that just happens to be stored along with many innocuous files inside the

---

78. See Katz v. United States, 389 U.S. 347, 353 (1967) (holding that electronic recording of a conversation in a telephone booth falls within the Fourth Amendment's scope); *Berger*, 388 U.S. at 64 (describing wiretapping as akin to "a trespassory invasion of the home or office"); Olmstead v. United States, 277 U.S. 438, 475–76 (1928) (Brandeis, J., dissenting) ("Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard.").

79. See Kyllo v. United States, 533 U.S. 27, 31 (2001) (noting that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no").

80. See, e.g., Maryland v. Garrison, 480 U.S. 79, 84 (1987).

81. See id.

82. *Garrison* notes these concerns:

> The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found.

Id. (internal citations and quotations omitted).

container of the computer hardware.[83] Under traditional rules, then, seizing computer hardware to get a handful of files would appear to be overbroad.[84] It's roughly analogous to seizing an entire house and carting off its contents to mine them for evidence of crime, which the Fourth Amendment prohibits.[85] The problem is that the traditional rule requires a level of surgical precision and expertise that is possible for physical evidence but not digital evidence. When Fred Felony robbed the physical bank, the police could obtain a warrant to search his home for the stolen bills and search the home in a few hours.[86] There was no need to cart off everything in the house and search it weeks or even months later in a laboratory. A rule requiring officers to look for the bills and retrieve only the bills named in the warrant is a sensible rule in such an environment. A computer search is different: It takes much more time, and may require considerable technical expertise. The approach that works for physical evidence does not work well for digital evidence.

Fast forward to the next stage, in which investigators generate a bitstream image of the seized computer. The need for legal regulation is clear. The imaging process allows the government to recreate its own perfect copy of everything on a suspect's computer. After obtaining their own copy, investigators have the technical ability to mine it for clues without limit. They can search through the copy for hours, weeks, or even

---

83. See Davis v. Gracey, 111 F.3d 1472, 1478–80 (10th Cir. 1997) (challenging search warrant for computer as overbroad and seizure of computer as illegal, on grounds that real evidence was merely a file contained on that computer).

84. In United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), the Ninth Circuit considered a factual situation similar to a modern search through computer files: a search for a single document hidden somewhere in many boxes of documents. Rather than search through the boxes and seize only the one document, investigators carted off all the documents to search them off-site at a later time. The Ninth Circuit condemned the practice:

> It is highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the fourth amendment. As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized. It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search. However, the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as the kind of investigatory dragnet that the fourth amendment was designed to prevent. We cannot sanction the procedure followed by the Government in this case.

Id. at 595 (internal citations and quotations omitted). I am assuming in this discussion that the hardware is not also evidence or an instrumentality of crime. Where that assumption is incorrect, the hardware can be independently seized. See *Davis*, 111 F.3d at 1480 (computer used to store obscene images); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (computer used to store child pornography).

85. See generally Kremen v. United States, 353 U.S. 346 (1957) (per curiam) (holding that the Fourth Amendment does not permit seizure of a house and removal of its contents for subsequent examination).

86. See supra notes 3–5 and accompanying text.

years. Remarkably, traditional Fourth Amendment rules appear to impose no limits on this process.[87] Under the traditional rules, copying a computer file does not "seize" it, and analysis of the government's copy would appear not to constitute a "search."[88] The problem is the traditional definition of seizure, which remains tied to the physical notion of depriving another of their property. A seizure occurs when a government official causes "meaningful interference with an individual's possessory interests in that property."[89] This test serves as a useful guide to limit interference with physical property, but it fails when applied to digital evidence.[90] Detectives no longer need to impose a meaningful interference on a possessory interest to obtain digital evidence. Because police can create a perfect copy of the evidence without depriving the suspect of property, the new facts unhinge the rule from its traditional function of limiting police investigations.[91]

At the final stage of the investigation, investigators look through the copy for evidence of the crime. This raises a threat to privacy that I call the needle-in-a-haystack problem. Because computers can store an extraordinary amount of information, the evidence of crime is akin to a needle hidden in an enormous electronic haystack. If no rules regulate how investigators look through the haystack to find the needle, any justification for a search may justify an invasive look through computer files that represent a small city's worth of private information. Existing Fourth

87. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (concluding that making a copy of computer data "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").

88. See Arizona v. Hicks, 480 U.S. 321, 324 (1987) (holding that copying a serial number does not constitute a seizure); United States v. Thomas, 613 F.2d 787, 793 (10th Cir. 1980) (holding that photocopying documents does not constitute a seizure because it is not a taking that involves dispossession).

89. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

90. Courts have hinted in some cases that they might adopt a different definition of seizure in the context of electronic evidence, but those cases generally arise in the quite different context of interpreting Federal Rule of Criminal Procedure 41. Rule 41 authorizes warrants to seize "property," and several cases have raised the question whether this authority allows the police to use Rule 41 to authorize electronic monitoring or conduct so-called "sneak and peek" warrants. In that context, the courts have suggested that it is a seizure of property to view or copy information. See United States v. N.Y. Tel. Co., 434 U.S. 159, 169 (1977) (stating that Rule 41 "is broad enough to encompass a 'search' designed to ascertain the use which is being made of a telephone suspected of being employed as a means of facilitating a criminal venture and the 'seizure' of evidence which the 'search' of the telephone produces"); United States v. Freitas, 800 F.2d 1451, 1455 (9th Cir. 1986) (holding that Rule 41 authorized a sneak and peek search in a case involving an illegal drug laboratory and that the property to be seized under the warrant "was information regarding the 'status of the suspected clandestine methamphetamine laboratory'").

91. See Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L. Rev. 39, 107 (2002) ("[T]he terms search and copy, as used with regard to electronic evidence, have different implications than the terms have in the physical world.").

Amendment rules have been developed to prevent this sort of general rummaging in searches for physical property. The place to be searched must be limited to a specific physical location, such as an apartment or an office, and the search must be objectively consistent with a search for the evidence named in the warrant.[92] The rules attempt to ensure that searches pursuant to warrants remain narrowly tailored to the government's interest.

These rules do little to regulate searches for electronic data, however. Digital evidence alters the relationship between the size of the space to be searched and the amount of information stored inside it. In physical space, the particularity requirement limits the scope of a search to a place on the order of a house or apartment. Limiting the space to be searched serves as a key limitation on the scope of the search.[93] That limitation does not hold in the case of a computer search. In late 2004, the hard drive on a typical new home computer stored at least forty gigabytes of information,[94] roughly equivalent to twenty million pages of text or about half the information stored in the books located on one floor of a typical academic library.[95] By the time you are reading this article, the capacity no doubt will have increased; the storage capacity of new hard drives has tended to double about every two years.[96] Given how

---

92. United States v. Van Dreel, 155 F.3d 902, 905 (7th Cir. 1998) ("[U]nder *Whren*, . . . once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant."); United States v. Ewain, 88 F.3d 689, 692–93 (9th Cir. 1996) (noting that "[o]nce the police are lawfully searching in a place for one thing, they may seize another that is in plain view, if its incriminating nature is immediately apparent").

93. As the Supreme Court suggested in *United States v. Ross*:

> Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to searcb an upstairs bedroom, prohable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.

456 U.S. 798, 824 (1982).

94. See, e.g., How to Buy A Desktop PC, at http://www.pcworld.com/bowto/bguide/0,guid,14,page,3,00.asp (last visited November 13, 2004) (on file with the *Columbia Law Review*).

95. See, e.g., How Much Text Is in a Kilobyte or Megabyte, at http://www.wisegeek.com/how-mucb-text-is-in-a-kilobyte-or-megabyte.htm (last visited November 18, 2004) (on file with the *Columbia Law Review*) (explaining conversions of bytes to pages of text); Megabytes, Gigabytes, Terabytes . . . What Are Tbey?, at http://www.pcsndreams.com/Pages/Articles/Megabytes.htm (last visited November 18, 2004) (on file with the *Columbia Law Review*) (comparing measures of data stored digitally to the physical space required to store the same amount of data printed on paper).

96. One can see this phenomenon in the rapidly outdated claims of how much storage space computer hard drives contain. See, e.g., Kevin J. Harrang, Licensing Issues in Creating and Publishing Multimedia Software Products, 418 PLI/Pat 289, 294 n.3 (1995) ("The typical hard disk of a personal computer . . . stores anywhere from about 40 to 400 megabytes of data."); Shira A. Scheindlin & Jeffrey Rabkin, Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?, 41 B.C. L. Rev. 327, 367 (2000) ("Hard

much information can be stored in a small computer hard drive, the particularity requirement no longer serves the function in electronic evidence cases that it serves in physical evidence cases. Whatever remaining function it serves diminishes every year. Today, limiting a search to a particular computer is something like limiting a search to a city block; ten years from now, it will be more like limiting a search to the entire city.

To some extent this problem was presaged by physical cases involving many boxes of paper documents. But searches for paper documents have not caused the same order of heartburn that searches for computer files will raise, and have not triggered new rules to address the needle-in-a-haystack problem. *Andresen v. Maryland* illustrates the dynamic.[97] In *Andresen*, police searched through paper files at a lawyer's office for evidence of fraud relating to a real estate transaction. The defendant objected that the warrant was insufficiently particular, but the Supreme Court easily approved the warrant. The Court found it sufficient to address the needle-in-a-baystack problem with only a general aside tucked away in a footnote: "We recognize that there are grave dangers" inherent in document searches, the Court explained.[98] "In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[99] The Court offered a warning but no legal rule to address this problem, stating only that "responsible officials . . . must take care to assure" that such searches "are conducted in a manner that minimizes unwarranted intrusions upon privacy."[100]

The lost functionality of the particularity requirement in digital evidence searches cannot be restored merely by requiring greater specificity. Existing technology simply gives us no way to know ahead of time where inside a computer a particular file or piece of information may be located. In the physical world, different spatial regions are used for different purposes. This allows the police to make educated guesses as to where evidence may or may not be found, which allows them to generate ways to limit the search. Consider the warrant obtained to search Fred Felony's bome in the physical-world bank robbery investigation. The warrant can be limited to Fred's home because he is unlikely to store evidence in the street or in a public park. In the computer context, however, the decision of where within a storage device to place particular information is determined primarily by the particular software installed and the contingent questions of what else happens to be stored on the

---

drives that store 3000 to 4000 megabytes (or three to four 'gigabytes') are commonplace.").

97. 427 U.S. 463 (1976).

98. Id. at 482 n.11.

99. Id.

100. Id.

same storage drive.[101] For the most part, this is impossible to know before the item is seized and analyzed at the government's lab.

Even in the controlled setting of a forensics lab, existing Fourth Amendment rules fail to generate useful guides to investigative conduct. Consider two potential legal limitations on the scope of the forensic analyst's search: first, limits on which regions of a hard drive the analyst can look for evidence named in the warrant, and second, limits on the analyst's ability to look for evidence of other crimes. The general Fourth Amendment rule is that investigators executing a warrant can look anywhere in the place to be searched where evidence described in the warrant might conceivably be located.[102] In traditional investigations for physical evidence, this rule means that officers cannot look in places smaller than the evidence they wish to seize. If the police have a warrant to recover a handgun, the warrant does not justify opening a personal letter. But electronic evidence can be located anywhere. Files can be mislabeled, hidden, or otherwise stored in a way that the investigator can never rule out a particular part of the hard drive ex ante.[103] As a result, officers can look through the entire digital haystack to find the needle.[104] The traditional rule imposes a substantial limit for physical searches, but not for searches for electronic evidence.

The same occurs with the rules that enforce the scope of the warrant. When evidence beyond the warrant is seized under the plain view exception, defendants routinely move to suppress that evidence on the ground that it was discovered in a search that exceeded the warrant's scope. Existing law calls on judges to ignore the officer's subjective intent to look for items beyond the warrant.[105] The doctrine asks instead whether the search that the officer actually conducted was objectively consistent with

---

101. See generally Nelson et al., supra note 20, at 73–158 (reviewing various types of file systems, structures, and storage).

102. United States v. Ross, 456 U.S. 798, 824 (1982).

103. See United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (noting that agents executing a search for computer files are "not required to accept as accurate any file name or suffix and [to] limit [their] search accordingly" because criminals may "intentionally mislabel files, or attempt to hury incriminating files within innocuously named directories"); United States v. Sissler, No. 1:90-CR-12, 1991 WL 239000, at *4 (W.D. Mich. Aug. 30, 1991) (stating that "the police were not obligated to give deference to the descriptive labels placed on the discs by [the defendant]. Otherwise, records of illicit activity could be shielded from seizure by simply placing an innocuous label on the computer disk containing them").

104. See United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) (stating that when searching computer data for information whose 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").

105. See United States v. Van Dreel, 155 F.3d 902, 905 (7th Cir. 1998) ("[U]nder *Whren*, . . . once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant."); United States v. Ewain, 88 F.3d 689, 694 (9th Cir. 1996) ("Using a subjective criterion would be inconsistent with *Horton*, and would make suppression depend too much on how the police tell their story, rather than on what they did.").

the kind of search that might reasonably be conducted for the evidence the warrant describes.[106] If it was, the unrelated evidence can be admitted under the plain view exception; if it was not, the evidence is suppressed. This rule appears plausible in the context of a search for physical evidence. An officer's subjective intent may be difficult to know, but it is generally possible to gauge whether an officer's steps are consistent with searches for particular types of evidence. A search for a stolen television might look different than a search for stolen paper bills. The rule does not impose a real limit on searches for electronic evidence, however. Because electronic evidence can be located anywhere on a hard drive, it is difficult, if not impossible, to say that a particular search was objectively unjustifiable. The physical-world rules do not prevent a general rummaging through electronic evidence.[107]

Finally, existing law imposes no time limits on computer searches and pays little attention to when or whether seized computers must be returned. Neither the Fourth Amendment nor the Federal Rules of Criminal Procedure require the police to begin the forensic examination process in a prompt way.[108] Once the computer has been seized, the police ordinarily can keep it indefinitely.[109] Federal law provides only a very limited mechanism for the return of property seized pursuant to a warrant;[110] the suspect must file a motion seeking a return of property and prove either that the seizure was illegal or that the government no

---

106. See *Van Dreel*, 155 F.3d at 905.

107. Cf. Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994) (describing the "intermingled documents problem" of Fourth Amendment jurisprudence and its relevance for computer searches). The problem is particularly significant because other digital files may support a more severe and more easily proven criminal charge. When searching through Fred's computer files, for example, agents would have a strong incentive to check to see if it happens to contain any images of child pornography. The possession of child pornography carries very high felony penalties. See, e.g., United States v. DeBeir, 186 F.3d 561, 567 (4th Cir. 1999) (calculating a sentence under U.S. Sentencing Guidelines). Smart investigators would know that if they find child pornograpby images on the hard drive, they could drop the bank theft charges against Fred and charge him with possessing child pornography instead. See, e.g., United States v. Carey, 172 F.3d 1268, 1273–74 (10th Cir. 1999) (discussing search through computer for drug-related evidence that led to child pornography charges); United States v. Turner, 169 F.3d 84, 86 (1st Cir. 1999) (explaining how a search through computer for evidence of assault led to child pornography charges); see also *Gray*, 78 F. Supp. 2d at 526–27 (explaining how search through computer for evidence of computer hacking led to child pornography charges).

108. United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (holding that Rule 41 does not "provide[ ] for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant").

109. See DOJ Manual, supra note 12, at 77 ("The government ordinarily may retain the seized computer and examine its contents in a careful and deliberate manner without legal restrictions . . . .").

110. Fed R. Crim. P. 41(g) ("A person aggrieved by . . . the deprivation of property may move for the property's return.").

longer has any need to retain the evidence.[111] If no motion is filed, the property need not be returned. Even if a motion is filed and granted, an order to return the computer does not require the police to return or destroy the bitstream copy they have generated.[112] Because the existing rule is focused on the suspect's property interest rather than a privacy interest, the police can keep the copy and continue to search it without apparent limit. Such rules may make sense for physical property but they show a surprising lack of attention to the legitimate interests that users have in their computers and files.

III. Toward New Rules of Criminal Procedure

Our constitutional tradition has tasked judges with implementing the Bill of Rights through specific rules. Those rules evolve in piecemeal fashion over time. In the case of the Fourth Amendment, judicial implementation has generated a complex doctrinal structure that fills several volumes in leading treatises.[113] That doctrine attempts to effectuate the Fourth Amendment's prohibition against "unreasonable searches and seizures" and the history of concern against general warrants through specific rules governing what law enforcement can and cannot do in specific situations.

Digital evidence exposes the contingency of the existing rules. It reveals how the rules generated to implement constitutional limits on evidence collection are premised on the dynamics of physical crimes and traditional forms of physical evidence and eyewitness testimony. When those implementing rules are applied to the facts of digital evidence collection, they no longer remain true to the purpose they were crafted to fulfill. Digital evidence changes the basic assumptions of the physical world that led to the prior rules, pointing to results that no longer reflect the basic goals and purposes of the Fourth Amendment.

In a narrow sense, this is nothing new. Evolution of the Fourth Amendment in response to technology is an old story, dating perhaps as far back as the first automobile exception case in 1925.[114] More recently,

---

111. See Ramsden v. United States, 2 F.3d 322, 326 (9th Cir. 1993) (stating that "[t]he United States' retention of the property generally is reasonable if it has a need for the property in an investigation or prosecution. However, 'if the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would become unreasonable" (quoting Fed. R. Crim. P. 41(e) advisory committee's notes (proposed amend. 1989))).

112. See id. at 327 (requiring government to return original set of documents but noting that it can keep a set of copies).

113. See, e.g., Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment (3d ed. 1996).

114. See Carroll v. United States, 267 U.S. 132, 149 (1925) (holding that an automobile can be searched without a warrant if probable cause exists to believe contraband was stored within it). The rule announced in *Carroll* was based, at least in part, on the technological reality of automobiles. A warrant requirement would not be practicable, the Court noted, "because the vehicle can be quickly moved out of the locality

the "reasonable expectation of privacy" test from *Katz v. United States* was designed to update the Fourth Amendment to help regulate telephone surveillance, and more broadly to achieve some kind of technology neutrality within search and seizure law.[115] Similarly, courts have seen cases involving paper documents for years.[116] All of this is true, but it only tells part of the story. While *Katz* emphasized the need for change, its impact on the law has been surprisingly narrow. *Katz* focused on only the preliminary question of what counts as a "search," and as I have shown elsewhere, has had surprisingly little effect on Fourth Amendment law as a whole.[117] In a similar vein, courts have not responded to searches for paper documents by generating new rules to regulate paper searches.[118] While cases involving telephones and paper documents introduced the conceptual shift from physical evidence to rawer forms of data, they are neither so common nor so different from traditional cases as to have triggered major shifts in the law of criminal procedure.

The increasing reliance on computers in almost every facet of American life raises quite different considerations. Jack Balkin has noted that when we think about the impact of new technologies on the law, the issue is not novelty but salience.[119] "What elements of the social world does a new technology make particularly salient that went relatively unnoticed before? . . . And what are the consequences . . . of making this aspect more important, more pervasive, or more central than it was before?"[120] We are no longer dealing with microphones taped to telephone booths or stacks of papers resting in file cabinets. Today a growing portion of our lives is conducted via the intermediary of computers. Digital evidence collection and analysis is becoming an increasingly routine and essential part of a broad array of criminal investigations. Our societal reliance on computers combines with the differences between physical evidence and digital evidence to generate a pressing need for a rethinking of the procedural rules that govern digital evidence collection.

Lawrence Lessig has argued that courts should engage in "translation" when they apply the Constitution to the internet.[121] Translation is

---

or jurisdiction in which the warrant must be sought." Id. at 153. The rule also appeared to factor in the social realities of automobile use in the Prohibition era. Probable cause was required, the Court suggested, because "[i]t would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search." Id. at 153–54.

115. 389 U.S. 347, 353 (1967).

116. See supra text accompanying notes 97–100.

117. See Kerr, New Technologies, supra note 32, at 807.

118. See supra notes 97–100 and accompanying text.

119. Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U. L. Rev. 1, 2 (2004).

120. Id. at 2–3.

121. See generally Lawrence Lessig, Code and Other Laws of Cyberspace (1999) [hereinafter Lessig, Code]; Lawrence Lessig, Fidelity as Translation, 71 Tex. L. Rev. 1165 (1993).

an effort to update rules of law in response to changing technologies and social practice.[122] It justifies altering doctrinal rules to ensure that the basic role and function of constitutional commands remain constant across time. For example, Lessig argues that the Fourth Amendment should be understood as a general command to protect privacy.[123] When applying the Fourth Amendment to the internet, he suggests, judges sbould adopt rules that protect privacy given the realities of how the internet works.[124] Lessig's approach offers interesting possibilities, but generates only a partial answer. While translation permits doctrinal evolution in response to changing technologies and social practices, it remains locked into preexisting institutional arrangements. It requires the courts to assume the role they have traditionally assumed and to take the lead in reshaping the rules in light of technological change.

A better approach is to open the possibilities of a new criminal procedure to new institutional arrangements. The courts should retain an important role: Where needed changes fit nicely into the traditional scope and purposes of Fourth Amendment rules, courts can retailor existing rules in light of new facts. But this evolutionary approach is only part of a broader response legal institutions can offer. Some of the new challenges raised by digital evidence map cleanly onto traditional Fourth Amendment principles; others may not. When they do not, legislatures and executive agencies can offer new and creative solutions to regulate digital evidence collection. While the judicial branch is limited by stare decisis, the legislative and executive branches can experiment with a wide range of approaches.[125] They can identify and enact new rules in response to the dynamics of new technologies. In addition, legislatures and executive agencies can regulate comprehensive solutions without waiting for cases and controversies to arise.[126] The greater flexibility of legislative and executive branch rulemaking suggests that we should not look only to the courts. As I recently have explained elsewhere, the judiciary's relative institutional difficulties in the regulation of developing technologies suggests that other branches should play an important role.[127] We should rethink the law and its purposes from first principles, looking beyond constitutional traditions that have functioned effectively in traditional cases but may not prove entirely adequate when applied to digital evidence.

This Part offers a few tentative thoughts about what solutions the legal system might adopt in response to the new facts of the three basic mechanisms of digital evidence collection. Its primary goal is to jump-

122. See Lessig, Code, supra note 121, at 114.

123. See id. at 115.

124. See id. at 115–16.

125. See Kerr, New Technologies, supra note 32, at 166–69 (noting different operative constraints of judicial and legislative branches).

126. See id. at 163–66.

127. See generally id.

start thinking about new solutions, rather than lay out detailed proposals. Its secondary goal is to show that such changes may have begun to occur already. A new set of rules applicable in computer crime investigations has begun to emerge. Both Congress and the courts already have altered several of the rules of criminal procedure in response to the new facts of computer crime investigations. Congress has been the primary actor at two stages: It has enacted rules to regulate both the subpoena process and prospective surveillance in ways that start to address future needs. The courts have been active in the third stage, involving the computer forensics process. The steps taken so far are modest. Some judicial measures are lower court proposals that may be reversed on appeal or weakened by future decisions, and some cut across the grain of other cases on the same question. Several of the legislative measures need considerable work. Taken together, however, these statutory and constitutional developments likely represent the beginning of a new branch of criminal procedure designed specifically to regulate digital evidence—a branch more responsive and institutionally diverse than the law that exists today.

A. *Collection of Stored Evidence from Third Parties*

Consider the initial step of most computer crime investigations, the collection of stored evidence from third-party service providers. The increase in the amount and importance of information stored with third parties in a network environment creates the need for new limits on the subpoena power. The most obvious limit would come in the form of a higher legal threshold to compel disclosure; the law should require a more burdensome factual showing to obtain private information about suspects, such as their personal e-mail. Other limits may be considered as well. Perhaps the law should limit the number of target accounts that can be compelled at any one time, at least absent special justification. Perhaps prior notice should be required in some cases, or targets of investigations should be informed within a period of time after the disclosure occurs. Use restrictions might be a good way to limit the dangers arising from otherwise broad disclosures. For example, the law might prohibit the government from using information compelled from a provider for a purpose unrelated to the initial disclosure. Alternatively, the government might be required to delete information after a period of time, perhaps thirty days. The new rules should respond to the new privacy threats raised by third-party possession of private information made commonplace by computer networks and the internet.

Although the courts have not made any steps toward such a regime, Congress has. Congress showed remarkable foresight by enacting rules to narrow the scope of the subpoena power as far back as 1986, when Congress passed the Electronic Communications Privacy Act.[128] In their current form, the rules limiting the subpoena power appear in 18 U.S.C.

128. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

§ 2703. Section 2703 imposes statutory restrictions on how the government can obtain information from ISPs. Although the statute remains poorly understood, it requires law enforcement to satisfy a higher showing than a subpoena to obtain private information relating to customers and subscribers of ISPs.[129] When investigators seek private information such as undelivered e-mails, they first must obtain a search warrant based on probable cause.[130] The statute imposes a lesser requirement of a "specific and articulable facts" court order to obtain some other information,[131] and also imposes a requirement of prior notice to the user in certain contexts.[132] I have explained this statute in detail elsewhere, and will not do so here.[133] The key is that Congress has stepped in and begun to address how the architecture of the new investigations should change the old rules. The statutory regime is not perfect, but it begins to return the law to something akin to the balance it reaches in traditional investigations.

B. *Prospective Surveillance*

The mechanisms of prospective surveillance also require a new legal regime. The most basic need is for the relevant legal thresholds to focus, to the extent possible based on existing technology, on the type of information to be collected rather than on whether the space to be entered is public or private. The rules should attempt to correlate the showing required to conduct surveillance with the degree of the privacy threat raised by that type of surveillance. When a filter is configured to collect information of a type that tends to be private, a high threshold should be required. In contrast, prospective surveillance should be allowed under a lower threshold when less private information is collected. This approach would require the law to classify internet communications based

---

129. I explain section 2703 in considerable depth in 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, 1218–20 (2004) [hereinafter Kerr, User's Guide].

130. 18 U.S.C. § 2703(a) (2000). This section states:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

Id.

131. Id. § 2703(d). The section states that:

> A court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction . . . and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Id.

132. Id. § 2703(b).

133. See generally Kerr, User's Guide, supra note 129.

on the degree of the privacy interests at stake. For example, it might work to have one category for very private materials such as e-mails, an intermediate category for information relating to websurfing habits, and a third threshold for low privacy information such as IP headers or hacker communications.

More creative options may be worth exploring as well. Prospective internet surveillance raises a needle-in-the-haystack problem: The filter must be set so that it picks up the needle but not the hay. A range of mechanisms exists to help focus the process. One option would be to adopt the minimization strategies from the Wiretap Act and apply them more broadly to all forms of prospective surveillance.[134] For example, the law might require neutral third parties to review evidence collected via prospective surveillance before it is passed on to law enforcement agents. Alternatively, the law could regulate the types of tools used to ensure that the most effective ones are used, or it might require logging or recordkeeping by those tools to create a record of how they are used. A few of these ideas were raised in the debate over the FBI's prospective surveillance program sometimes known as Carnivore;[135] the same questions should be asked more broadly about any method of prospective surveillance.

Congress has made a few tentative steps in such a direction already, albeit not without inviting considerable controversy. The USA Patriot Act of 2001 (Patriot Act) amended the Electronic Communications Privacy Act by dividing prospective surveillance into two categories.[136] The first category is prospective surveillance of "contents" of communications,[137] and the second is the prospective surveillance of "dialing, routing, addressing, or signaling information" (DRAS).[138] The former is the more

134. See 18 U.S.C. § 2518. See generally United States v. Scott, 504 F.2d 194, 198–99 (1974) (discussing section 2518's minimization requirements in context of telephone wiretap).

135. See, e.g., IIT Research Inst., Independent Technical Review of the Carnivore System Draft Report (2000), available at http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf (on file with the *Columbia Law Review*); IIT Research Inst., Independent Technical Review of the Carnivore System Final Report (2000), available at http://www.usdoj.gov:80/jmd/publications/carniv_final.pdf (on file with the *Columbia Law Review*) (emphasizing need for postcollection auditing of uses of Carnivore).

136. See generally Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, § 216, Pub. L. No. 107-56, 115 Stat. 272, 288–90 (amending generally 18 U.S.C. §§ 3121–3127).

137. See 18 U.S.C. § 2510(8) (defining "contents" for wire or electronic communication as that which "includes any information concerning the substance, purport, or meaning of that communication"). This provision was enacted in 1968 and amended in 1986. See Kerr, Internet Surveillance, supra note 10, at 647 n.194.

138. See 18 U.S.C. §§ 3127(3)–3127(4) (Supp. 2002) (defining pen registers and trap and trace devices as devices that record, decode, or capture "dialing, routing, addressing and signaling information"). As I have noted elsewhere, the structure here is awkward for historical reasons: Rather than regulate noncontent prospective surveillance directly, the statute prohibits particular devices and then defines them as devices that conduct

private category of communication: Although its scope is not entirely clear,[139] it includes the contents of e-mails and probably the text of internet commands[140] and search terms.[141] The latter is the less private category of communications, including internet packet headers, e-mail addresses, and other data used for routing internet communications (and, presumably, anything else that is not contents).[142] Under the Patriot Act, prospective surveillance that collects only DRAS is regulated by the low-protection Pen Register Statute.[143] The police need to obtain only a relevance court order to conduct surveillance, or fit the monitoring within one of several broad statutory exceptions.[144] In contrast, prospective surveillance that collects contents is regulated by the high-protection Wiretap Act.[145] The police must obtain a "super" search warrant before conducting surveillance, or else fit their conduct within one of several relatively narrow statutory exceptions.[146] The Patriot Act also adds a reporting requirement that in some contexts requires law enforcement agencies to file reports on the use of prospective surveillance with the court that authorized the surveillance.[147]

The Patriot Act includes another innovation: It adds an exception to the Wiretap Act to exempt the communications of computer hackers sent through a victim's computer.[148] Under this provision, a victim of hacking can allow law enforcement to conduct prospective surveillance of a hacker's communications if there are "reasonable grounds to believe that the contents of the computer trespasser's communications will be rele-

---

noncontent prospective surveillance. See Kerr, Internet Surveillance, supra note 10, at 638 n.149.

139. See Kerr, Internet Surveillance, supra note 10, at 645–48.

140. See United States Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000).

141. In re Pharmatrak Inc., 329 F.3d 9, 18–19 (1st Cir. 2003).

142. See Kerr, Internet Surveillance, supra note 10, at 644–48 (describing status of these data in statutory surveillance regimes).

143. 18 U.S.C. §§ 3121–3127 (Supp. 2002); see DOJ Manual, supra note 12, at 111–12.

144. Section 3121(h) lists the exceptions, which include monitoring conducted in the following circumstances:

> (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
>
> (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
>
> (3) where the consent of the user of that service has been obtained.

18 U.S.C. § 3121(b) (2000).

145. Id. §§ 2510–2522.

146. See generally DOJ Manual, supra note 12, at 116–41 (describing protection of the Wiretap Act and its exceptions).

147. 18 U.S.C. § 3123(a)(3)(A) (Supp. 2002).

148. See 18 U.S.C. §§ 2510(21), 2511(2)(i) (Supp. 2002). See generally Kerr, Internet Surveillance, supra note 10, at 658–71.

vant to [an] investigation."[149] Fred's online bank theft provides an example. If representatives of the public library used as an intermediary victim consented, the detective could set up prospective content surveillance at the library computer limited to monitoring Fred's future intrusions. If Fred hacked into the library computer again, the government would be able to monitor Fred's communications without first obtaining a warrant. The idea behind the so-called trespasser exception is to tailor surveillance rules to the privacy interest in internet communications. Because a computer hacker has no reasonable expectation of privacy in his illegitimate communications, the government should not be required to obtain a warrant to monitor a hacker's communications with the consent of the victim.[150]

The Patriot Act's approach to prospective surveillance is not without its flaws. Several of its rules are unclear, and some are poorly drafted.[151] But the basic concept is sound; the rules make a first step toward updating the law so that it better reflects the new dynamics of computer network prospective surveillance.

C. *The Computer Forensics Process*

The computer forensics process also needs a regime of rules tailored to the privacy threats and needs raised by modern uses of computers. On the one hand, the law should respect technological limitations of existing search methods and techniques. On the other hand, the rules should look beyond the traditional dynamic of regulating searches and seizure to counterbalance the burden that such technical limitations may impose. For example, if technical needs require off-site searches of seized computers, then off-site searches should be allowed. But the law need not stop there. The Federal Rules of Criminal Procedure could be amended to require investigators to begin the forensic analysis of seized computers promptly, and to return computers that do not contain evidence within a reasonable period of time. The rules might provide an explicit mechanism allowing suspects to stipulate that a mirror image of their computers is accurate and then enjoy a right to have their computer returned within a specific period of time.[152] The rules might also require that investiga-

149. 18 U.S.C. § 2511(2)(i)(III) (Supp. 2002).

150. See Orin S. Kerr, Are We Overprotecting Code? Thoughts on First-Generation Internet Law, 57 Wash. & Lee L. Rev. 1287, 1298–1300 (2000) (discussing difficulties created by applying Title III's "one-size-fits-all" approach to variety of internet communications).

151. For example, existing law does not make clear the precise scope of "contents" versus "DRAS," or even whether there is a third category of communication outside these two categories. Kerr, Internet Surveillance, supra note 10, at 644–48, 645 n.186. It also defines the scope of the trespasser exception using sloppy language. Id. at 667–69.

152. Of course, exceptions would be required for cases involving computerized contraband such as images of child pornography, as the equipment used to commit child pornography is subject to forfeiture provisions. See 18 U.S.C. § 2253 (2000) (criminal forfeiture); id. § 2254 (civil forfeiture); cf. United States v. Hill, 322 F. Supp. 2d 1081,

tors erase any copies of seized files when a criminal case has been closed, or at the very least bar investigators from opening or reviewing seized computer files after that point absent special court authorization. Taken as a whole, such changes would attempt to balance law enforcement needs and individual rights in property and privacy in light of existing technological realities.[153]

We can also think creatively about the rules that regulate the examination process itself. For example, one way to handle the digital needle-in-a-haystack problem would be to reject the plain view rule in the context of digital evidence searches. Under the plain view doctrine, investigators can seize evidence unrelated to the search when they come across it in the course of a valid search and its incriminating nature is immediately apparent. Because computers often must be searched comprehensively to locate the evidence sought, the plain view rule threatens to collapse the distinction between particular and general warrants. A particular warrant in theory may become a general warrant in practice, as all of the evidence in the computer may come into plain view during the course of the forensic analysis. Abolishing the plain view doctrine in computer searches would address this problem. Whether announced by the courts or crafted by Congress, a rule that digital evidence discovered beyond the scope of a warrant is inadmissible would eliminate any incentive to turn a targeted search into a fishing expedition.

While no changes this dramatic have occurred in either courts or Congress, there have been interesting signs of change in the courts. Some judges have begun to create a new set of distinct Fourth Amendment rules that attempt to respond to the shift from physical evidence to electronic evidence. A few of those changes already are widespread; others are just beginning to emerge. Some are outliers when considered amidst the body of law as a whole. But the key is that judges are beginning to bend the rules in response to the new facts of the computer forensics process. A number of judges have concluded that computer searches are "special,"[154] "unique,"[155] and "different,"[156] and are looking for new rules of criminal procedure that restore the function of the old rules given the new facts.

The best-established new rule is that investigators may seize the target's computer and take it off-site for later review. Although somewhat

---

1091–92 (C.D. Cal. 2004) (Kozinski, J., by designation) (holding that defendant has right to independent inspection of child pornography evidence, despite government's objections that material should not be allowed to be copied due to potential dissemination).

153. Cf. James M. Rosenbaum, In Defense of the Hard Drive, 4 Green Bag 2d 169, 171 (2001) (suggesting rules that might limit authority of employers to search employee computers, including a time-out period combined with prior notice).

154. United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).

155. United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930, at *4 (D. Utah Apr. 12, 2001).

156. People v. Gall, 30 P.3d 145, 156 (Colo. 2001) (Martinez, J., dissenting).

inconsistent with the traditional rule that investigators cannot seize property beyond the scope of probable cause, courts have uniformly approved this practice on grounds of practicality. It takes too long and requires too much expertise to search a computer on site, judges have noted.[157] Seizure of an entire computer passes constitutional muster because "[a]s a practical matter, the seizure and off-site search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain [the evidence.]"[158] The alternatives are impractical, and therefore not constitutionally compelled; it would not be reasonable "to have required the officers to sift through the . . . computer files found in [the defendant's] office, in an effort to segregate [those materials] that were outside the warrant."[159] Such concerns are hardly foreign to Fourth Amendment law, of course. The reasonableness aspect of the Fourth Amendment has permitted similar flexibility in other more traditional contexts.[160] But the practices have ossified gradually into a new Fourth Amendment rule: A valid warrant entitles investigators to seize computers and search them off-site at a later date.

While courts have loosened the traditional rules to allow off-site searches, some have also tightened the rules to try to limit the forensics process and avoid general rummaging through seized computers. For example, a number of federal magistrate judges have begun to issue warrants to search computers only on the condition that the government follows special restrictions on the subsequent search. Some judges have required the government to search the computer within a specific time frame and to return the computer to the suspect in a timely manner if no evidence is found.[161]

---

157. See *Hill*, 322 F. Supp. 2d at 1089–90 (noting time required to search a computer without damaging it).

158. United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

159. United States v. Henson, 848 F.2d 1374, 1383–84 (6th Cir. 1988); see also United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997), aff'd 178 F.3d 1281 (3d Cir. 1999) ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant . . . .").

160. For example, in Illinois v. McArthur, 531 U.S. 326 (2001), the Supreme Court held that the police could seize a man to stop him from entering his home because the police reasonably believed that he was going to destroy evidence inside and the police were in the process of obtaining a warrant. According to the Court, the seizure of the man was permissible because "[i]t involve[d] a plausible claim of specially pressing or urgent law enforcement need, *i.e.*, 'exigent circumstances.'" Id. at 331.

161. According to the DOJ Manual:

> Several magistrate judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days. Some magistrate judges have imposed time limits as short as seven days, and several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under

A recent case from Chicago suggests that some judges are taking bolder steps.[162] In *In re Search of 3817 W. West End*, a magistrate judge refused the government's request for a warrant to search a home computer unless the government first agreed to abide by preapproved computer search protocol outlining the steps that would be taken to locate the evidence stored in the hard drive.[163] The target of the search was suspected of engaging in tax fraud, and investigators established probable cause to believe that there was evidence of the crime on her home computer. The judge refused to allow the search of her computer without a specific judge-approved search protocol, however, arguing that doing so would grant the investigators "a license to roam through everything in the computer without limitation and without standards."[164] The judge justified the condition on four practical concerns: the fact that computers are seized first and searched at a later time; the likelihood that evidence of crime was commingled with unrelated and innocent files; the fact that computers can store a tremendous amount of information; and the existence of technical methods to refine searches.[165] In light of these practical concerns, the judge reasoned, the particularity requirement compelled preapproval of the search methods to ensure that the search was constitutionally reasonable.[166]

Courts also have altered rules that monitor when a search exceeds the scope of the warrant. No court has eliminated the plain view rule entirely, but at least two courts have narrowed it in practice by focusing on the investigator's subjective intent. The general rule is that an officer's subjective intent to veer outside a warrant does not matter; as noted earlier, this rule makes it difficult for courts to tell whether a computer search was narrowly tailored.[167] Two courts have responded to this difficulty by changing the rule in computer search cases. In *United States*

---

the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time.

DOJ Manual, supra note 12, at 77.

162. In re Search of 3817 W. West End, 321 F. Supp. 2d. 953 (N.D. Ill. 2004).

163. Id. at 955–56.

164. Id. at 962.

165. Id. at 958–59.

166. Other courts have suggested similar approaches. See, e.g., United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (suggesting that magistrate judge's authorization of search supported by affidavit that explained need for off-site search of computer constituted "the magistrate judge's authorization" of off-site search); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000) (suggesting that magistrate judge should approve search strategy for search of a computer); People v. Gall, 30 P.3d 145, 166 (Colo. 2001) (Martinez, J., dissenting) (arguing for a new Fourth Amendment rule governing search of computers "to properly protect privacy concerns inherent in the complex nature of computers"). Of course, these approaches are somewhat difficult to square with traditional doctrine. That doctrine requires the government to specify the place to be searched and the item for which to search, but traditionally has not been understood as requiring an explanation of how the search is to be executed.

167. See supra notes 90–92 and accompanying text.

v. Carey, an investigator searching through a seized hard drive for evidence relating to cocaine came across images of child pornography. The investigator stopped searching for narcotics-related evidence and spent the next several hours searching for images of child pornography.[168] The Tenth Circuit ruled that the officer's subjective intent governed: Because the officer changed the focus of his search from one type of evidence to another, the discovery of the evidence beyond the scope of the warrant was impermissible and the evidence was suppressed.[169] Similarly, in *United States v. Gray*, an investigator looking through a seized hard drive pursuant to a warrant for evidence of computer hacking came across an image of child pornography.[170] The investigator continued to look for hacking evidence, but noted additional images of child pornography that he discovered along the way.[171] The court upheld the admissibility of the child pornography, holding that the investigator's subjective intent kept the search within the scope of the warrant.[172] Under *Carey* and *Gray*, the plain view rule effectively has a new limit in computer cases: It allows the seizure of evidence outside the warrant only if it was uncovered pursuant to a good faith search for evidence described in the warrant. The new rule tries to restore some of the functionality of the old one given the new facts of the computer forensics process.

CONCLUSION

Changes in technology often trigger changes in law. Legal rules evolve in response to changes in the underlying facts. Given our heavy reliance on computers and the specific ways they operate, the use of computers in criminal activity poses significant challenges for traditional rules of criminal procedure. By substituting the gathering of digital evidence for the collection of physical evidence and eyewitness testimony, investigations involving computers replace traditional mechanisms of search and seizure with quite different forms of surveillance and new forms of forensic analysis. The law naturally will change in response. Although some changes will come from the courts in the form of a slow evolution of doctrinal rules, others should follow from a rethinking of the best rules to regulate digital collection and the best institutions to generate and implement those rules. The problem of digital evidence should inspire the creation of a new criminal procedure, a set of rules that both builds upon and expands from traditional solutions to embrace new and creative mechanisms for regulating evidence collection and use.

We should also recognize that the problem of digital evidence extends beyond our borders, and that helpful solutions and insights may be found there. Every industrial country is undergoing the same shifts from

168. 172 F.3d 1268, 1271 (10th Cir. 1999).
169. Id. at 1274.
170. 78 F. Supp. 2d 524 (E.D. Va. 1999).
171. Id. at 527.
172. Id. at 529.

physical evidence and eyewitness testimony to digital evidence that is occurring in the United States. We all use the same networks, the same hardware, and the same software. Although different countries have different constitutional traditions and protect different values, all are facing the same basic questions of how to regulate third-party evidence collection, prospective surveillance, and the computer forensics process. By looking broadly for new institutional arrangements and approaches to regulate digital evidence collection, we can open ourselves to the best ideas abroad to supplement the solutions generated from within our constitutional traditions.