Chapter 1

Approaching the Fourth Amendment

§ 1.1. Fourth Amendment text

The Fourth Amendment provides:

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

§ 1.2. Analytical structure of all Fourth Amendment questions

In analyzing any case involving a Fourth Amendment claim, three separate questions must be answered. First, is the Amendment applicable? The applicability question, in

turn, is a two—sided inquiry: (a) does the governmental activity—which must be either a search or a seizure—invade (b) an individual interest protected by the Amendment? If the Amendment does not apply, that ends the inquiry; it does not matter if the governmental actions are reasonable or not.[1] Second, if the Amendment does apply, is it satisfied? If it is found that the Amendment is applicable but not satisfied, a third question must be answered: what is the remedy, if any, for the violation? That third question is *not* a Fourth Amendment issue, given that the Supreme Court has, since 1974, stated that the exclusionary rule is not constitutionally mandated. This book is structured to provide detailed analysis of these three questions. An overview is offered here.

§ 1.2.1. Applicability

Defining a search or a seizure is a two-sided inquiry: governmental actions must invade a protected interest of the individual. If the individual does not have a protected interest, actions that might otherwise be labeled a search or seizure do not implicate the Fourth Amendment. If a person has a protected interest, then the applicability question turns on whether the governmental techniques used to obtain tangible things or information are considered searches or seizures.

§ 1.2.1.1. Governmental activity: searches and seizures

The Fourth Amendment is applicable only to governmental activity; it does not regulate private searches and seizures. As a consequence, a rather complex jurisprudence has developed to distinguish between governmental searches and private party searches.[2] Moreover, the Amendment applies to only two types of governmental activity: searches and seizures. These terms are not self-defining. Given the countless number of daily encounters between citizens and law enforcement officials,[3] this applicability question is one of the most common constitutional questions. It is also fundamentally important to decide cases in court and to guide police officers and individuals in determining how they may permissibly interact.

§ 1.2.1.1.1. Searches

The word "search" is a term of art in Fourth Amendment jurisprudence and is not used in its ordinary sense. Chapter 7 examines the various governmental methods of obtaining tangible things or information that are considered to be searches within the meaning of the Fourth Amendment. The conclusion that a search has occurred varies depending on the type of governmental activity utilized to obtain the evidence. That activity may include physical manipulation, visual observation, or other use of the senses, as well as the employment of instrumentalities such as a dog's nose or technological devices. In Supreme Court jurisprudence, physical manipulation by the police comes closest to a common sense understanding of what is a search. That literal view must be contrasted with other

1. The classic analysis of this point is in Charles E. Moylan, Jr., *The Fourth Amendment Inapplicable vs. The Fourth Amendment Satisfied: The Neglected Threshold of "So What?,"* 1977 S. Ill. L.J. 75. Judge Moylan often emphasized the same point in his opinions for the Court of Special Appeals of Maryland. *E.g.*, Brummell v. State, 685 A.2d 835 (Md. Ct. Spec. App. 1996).

2. *See* § 7.6.

3. *E.g.*, United States v. Aukai, 497 F.3d 955 (9th Cir. 2007) (en banc) (noting that there are 700 million airline passengers boarding commercial flights in the United States each year).

situations, particularly those involving sense-enhancing devices, where the legal definition is divorced from the ordinary meaning of the term, thus permitting the Court to conclude that no search has occurred. The use of technological devices to learn something that otherwise would not be discovered is so rapidly expanding that it is difficult to grasp the myriad ways the government can obtain tangible evidence or information. Unfortunately, the Court has not provided a comprehensive definition of the concept of a search to ascertain when the Amendment is implicated by a device that the government employs.

The search analysis is structured as follows:

- Types of government activity that may or may not be a search, including:
  - physical invasions, including plain feel § 7.3.
  - visual observations, including plain view § 7.4.2.
  - non-tactile searches § 7.4.
  - use of trained dogs § 7.4.3.2.
  - chemical field testing § 7.5.3.
  - technological enhancements to the senses § 7.4.1.4.
  - possible considerations to define a search § 7.5.
- Types of searches examined include:
  - automobile searches — probable caused based § 10.1.
  - community caretaking § 10.3.
  - consent § 10.4.
  - entrance-way searches § 10.5.
  - exigent circumstances § 10.6.
  - fire fighting and fire investigations § 10.7.
  - frisks/protective searches § 9.1.
  - international border and its functional equivalent § 10.2.
  - inventory searches § 10.8.
  - plain view § 7.4.2.4./plain feel § 7.3.1./plain smell § 7.4.3.1.
  - protective sweeps § 9.2.
  - search incident to arrest — Chapter 8
  - subpoenas duces tecum § 11.9.

§ 1.2.1.1.2. Seizures

§ 1.2.1.1.2.1. Seizures of persons

The Supreme Court's attempts to define a seizure of a person are of surprisingly recent vintage. Only in 1968 did it confront the issue directly for the first time. That case, *Terry v. Ohio*,[4] remains viable today as a basic source of understanding what the concept of a seizure means. In *Terry*, Officer McFadden was walking his beat when he observed three men whom he believed were planning to rob a store. He approached them, identified himself as a police officer, and asked their names. When one of the men, Terry, "mumbled something" in reply, the officer grabbed Terry and patted down the outside of his clothing, ultimately recovering a pistol. Recognizing that the Fourth Amendment applied when the officer took hold of Terry and patted down the outer surfaces of his clothing, the Court provided a broadly-stated view of a seizure: "Whenever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person."

4. 392 U.S. 1 (1968).

This definition, which is used repeatedly in later cases, involves two elements: accosting and restraint of freedom. The *Terry* Court noted, however, that "[o]nly when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen may we conclude that a 'seizure' has occurred." Thus, beginning with its first effort to define a seizure, the Court recognized two ways in which an officer can seize a person: by physical force or by show of authority. Adding precision to these two concepts in subsequent cases has proven to be difficult and controversial. Although the Court has since comprehensively — and more concretely — defined the concept of a seizure, it has continued to recognize that a seizure only results from either the application of physical force or through a show of authority.

After *Terry*, the Court eventually settled on the "reasonable person" test to define a seizure, which focused on the objective aspects of the encounter's effect on the mind of a reasonable person and asked the question whether a reasonable person would feel free to leave. That test was widely viewed as implicating the Fourth Amendment early in the encounter, focusing exclusively on the coercive nature of the police officer's words or conduct. A citizen's reaction to that coercive activity was immaterial.

In 1991, in *California v. Hodari D.*,[5] the Supreme Court redefined the concept of a seizure. That case establishes that a seizure occurs only when a suspect submits to a show of authority or is physically touched by law enforcement officials, who do so with the intent to seize. A seizure may result in either a stop or an arrest but it may only occur in one of those two ways. Seizures from physical contact require two elements: touching and an intent to seize, with that intent measured objectively. In the vast majority of cases involving physical restraint, the question whether an intent accompanied that restraint is obvious and no extended analysis is needed. Show of authority seizures also require two elements: a show of authority and submission. The submission must be in response to a show of authority that a reasonable person would interpret as a demonstration of the officer's intent to seize. Show of authority seizures require determining if, when, and how the person accosted submits. If the suspect responds inappropriately to a specific command, that response may not be considered submission or a fruit of that command. There has now developed a substantial body of case law and commentary addressing the implications of the *Hodari D.* definition. The case law demonstrates that the police have adapted their tactics to take advantage of that definition, resulting in a dramatic shift in the Fourth Amendment balance between individual security and law enforcement in favor of the police.

- The seizure of a person analysis is structured as follows:
  - overview of current analysis § 5.1.1.1.
  - nature of the interest implicated by a seizure § 5.1.1.2.
  - the variety of police/citizen encounters § 5.1.1.3.
  - initial views of the concept of a seizure § 5.1.2.
  - seizures involving physical contact § 5.1.3.
  - show of authority seizures, including the reasonable person test and requirement of submission § 5.1.4.
  - detainee responses to a seizure, including abandonment and inappropriate responses and flight as ending an initial seizure § 5.1.5.
  - attempted acquisition of control: a proposed definition of a seizure § 5.1.6.

5. 499 U.S. 621 (1991).

- Types of seizures of persons:
  - arrests § 6.3.
  - stops and distinguishing them from arrests, including permissible investigative techniques during a stop § 6.4.
  - traffic stops § 6.4.3.
  - roadblocks and checkpoints § 6.5.
  - detentions during execution of search warrants § 6.6.
  - detentions of material witnesses § 6.7.

§ 1.2.1.1.2.2. Seizures of property

To determine if a seizure of property has occurred, the nature of the governmental conduct and the nature and scope of the individual's interest are examined. The Court has often repeated the following definition: a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[6] It has sometimes also stated that a seizure "deprives the individual of dominion over his or her property."[7] One could question whether such definitions adequately convey the full nature of the individual's interests implicated by a seizure and some observations regarding that matter are offered.[8] Nonetheless, the Court's inquiry has focused on possession and lower court opinions relentlessly reflect that focus.[9]

Unlike seizures of persons, seizures of property have generated comparatively little Supreme Court case law and the definition has been relatively stable. Most seizures of property are obvious takings of physical possession and require little analysis. There are some situations where a property seizure is not so patent, including those in which the property is in transit and unaccompanied by the owner. Other conceptual problems include using the Supreme Court's definition of a seizure of property in cases involving the acquisition of digital evidence or other intangible property.

- The following aspects of property seizures are examined:
  - physical seizures of material property § 5.2.2.
  - tracking devices as seizures § 5.2.3.
  - intangible property and digital evidence § 5.2.4.
  - protected interests in property in addition to possession § 5.2.5.

§ 1.2.1.2. Protected individual interests

Governmental activity that would otherwise constitute a search or a seizure must invade an interest of a person protected by the Amendment in order for the Amendment

6. United States v. Jacobsen, 466 U.S. 109, 114 (1984). *Jacobsen* observed that, although "the concept of a 'seizure' of property is not much discussed in our cases, this definition follows from our oft-repeated definition of the 'seizure' of a person within the meaning of the Fourth Amendment—meaningful interference, however brief, with an individual's freedom of movement." *Id.* at 114 n.5.

7. Horton v. California, 496 U.S. 128, 133 (1990).

8. *See* § 5.2.5.

9. Once it is established that a seizure has occurred, it must be justified as reasonable. *See* Chapter 11. Consistent with the treatment of seizures of persons, the Court has distinguished between temporary detentions, justified by articulable suspicion, and longer detentions, for which a probable cause-based warrant is needed. *E.g.*, United States v. Place, 462 U.S. 696 (1983) (adopting two levels of justification for seizures of effects).

to be applicable. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects." There are two aspects to the analysis of this provision: what objects are protected; and to what extent is each object protected? Grammatically, there is a relational aspect to the right set forth in the Amendment, which speaks of certain objects protected — people, houses, papers, and effects. But those objects are not absolutely shielded. Instead, the right to be "secure" is protected. If one does not know what is protected by the Amendment, then it cannot be determined what the government can do without implicating it. If one does know what is protected, governmental intrusions of that protected interest must be analyzed to determine whether they are considered a search or seizure and accordingly justified as reasonable. As one distinguished commentator has observed: "The key to the Amendment is the question of what interests it protects."[10]

Currently, according to the Supreme Court, "[e]xpectations of privacy and property interests govern the analysis of Fourth Amendment search and seizure claims."[11] Following that command, one must distinguish between searches and seizures. Seizures of property implicate a person's right to possess it; seizures of persons implicate that person's liberty and freedom of movement; and searches implicate a person's reasonable expectation of privacy. As a consequence, it must be determined which individual interest has been affected by the governmental action. To illustrate, although mere passengers in an automobile ordinarily have no recognized reasonable expectation of privacy impacted by a search of the vehicle,[12] they do have a right to challenge the stop of a vehicle in which they are riding because they are seized when the vehicle is stopped.[13]

The Supreme Court initially grounded Fourth Amendment protections in common law property concepts. Pursuant to that property-based analysis, the Court created a hierarchy of property rights and restricted the ability of the government to search and seize to only those situations where the government had a superior property right. It also used property concepts to limit the protections of the Amendment to the physical aspects of the four objects listed in the Amendment, dividing the world into areas that were constitutionally protected and those that were not. Those property-based theories were repudiated by the Court in *Warden v. Hayden*[14] and *Katz v. United States*.[15]

The Court in the last third of the twentieth century adopted and generally still employs the reasonable expectation of privacy test to define, in large part, the right to be secure. To have a protected interest, that two-pronged test requires that a person exhibit a subjective expectation of privacy, which must be recognized by society as reasonable. Pursuant to that test, the Court has created a hierarchy of expectations, with long lists of situations where it has found either no reasonable expectation of privacy or a reduced one. If no reasonable expectation of privacy is found (and no other protected interest is present), the Amendment is inapplicable to regulate the government action. If the Court finds a reduced expectation of privacy, the governmental intrusion has been almost uniformly upheld, with the Court utilizing a test for reasonableness favorable to the government.

As the reasonable expectation of privacy test has demonstrated its limitations, the Court has sometimes looked beyond that approach to find other values that animate the

10. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 385 (1974).
11. United States v. Padilla, 508 U.S. 77, 82 (1993) (per curiam).
12. Rakas v. Illinois, 439 U.S. 128 (1978).
13. Brendlin v. California, 551 U.S. 249 (2007).
14. 387 U.S. 294, 315 (1967).
15. 389 U.S. 347 (1967).

right to be secure. Now, the Court recognizes that the Amendment protects certain property interests as such, as well as possessory and liberty interests. Hence, although the Court in adopting the expectations test emphatically rejected a property-based analysis, that ground has regained viability. The home has a special status as a protected place,[16] even when the owner is not present.[17] Indeed, the physical entry into the home has been described as the "chief evil against which the wording of the Fourth Amendment is directed."[18]

As to the person's right to be secure from an unreasonable seizure, that interest has been variously described as the right to be left alone,[19] individual freedom,[20] the "inviolability of the person,"[21] and the right of free movement.[22] In *Terry v. Ohio*,[23] which involved the stop and frisk of a person, the Court emphasized the words chosen by the Framers to define the nature of the interest protected, asserting that the "inestimable right of personal *security* belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs." Indeed, the Court said: "'No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.'"

As to effects, the Court has clearly distinguished one other protected interest in addition to privacy, that is, the individual's possessory interest in an object.[24] This has occurred in the context of distinguishing between searches and seizures: although a search implicates privacy concerns, a seizure implicates the person's interest in retaining possession of his or her property.[25]

There are other indications of a broader meaning to the concept of security. Indeed, although often unstated in Supreme Court opinions, the essential attribute of the right to be secure is the ability of the individual to exclude the government from unreasonably searching or seizing one's person, house, papers, and effects. Without the ability to exclude, a person has no security. With the ability to exclude, a person has all that the Fourth Amendment promises: protection against unjustified intrusions by the government.[26]

---

16. *E.g.*, Florida v. Jardines, 569 U.S. __, 133 S. Ct. 1409 (2013); Kyllo v. United States, 533 U.S. 27 (2001).

17. Alderman v. United States, 394 U.S. 165, 176 (1969).

18. United States v. United States Dist. Court, 407 U.S. 297, 313 (1972). *Accord* Welsh v. Wisconsin, 466 U.S. 740, 748 (1984); Payton v. New York, 445 U.S. 573, 585 (1980).

19. *See, e.g.*, Wilson v. Schnettler, 365 U.S. 381, 394 (1961) (Douglas, J., dissenting) ("Under the Fourth Amendment, the judiciary has a special duty of protecting the right of the people to be let alone. . . ."). *But see* Katz v. United States, 389 U.S. 347 (1967) (the Fourth Amendment is not coextensive with any right to be left alone).

20. *See, e.g.*, Ker v. California, 374 U.S. 23, 32 (1963) ("Implicit in the Fourth Amendment's protection from unreasonable searches and seizures is its recognition of individual freedom.").

21. Wong Sun v. United States, 371 U.S. 471, 484 (1963).

22. *See, e.g.*, Maryland v. Wilson, 519 U.S. 408, 412–13 (1997) (discussing driver's and passenger's liberty interests when a police officer orders them out of a lawfully stopped car); Michigan v. Chesternut, 486 U.S. 567, 573 (1988) (seizure occurs when a reasonable person concludes he is not free to leave); United States v. Martinez-Fuerte, 428 U.S. 543, 557–58 (1976) (routine traffic stop may intrude on a motorist's right to uninterrupted free passage).

23. 392 U.S. 1 (1968).

24. *See* Horton v. California, 496 U.S. 128, 134 (1990) (seizure of article in plain view does not involve invasion of privacy but does invade owner's possessory interest).

25. United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed," whereas "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property").

26. *See* § 3.4.4.

The Fourth Amendment provides that the right of the people to be secure against unreasonable searches and seizures applies to four specified objects — persons, houses, papers, and effects. The government can intrude into any non-protected item at will because the Fourth Amendment is inapplicable.[27] Interpreting the Amendment literally, the Court in *Olmstead v. United States*[28] and its progeny divided the country into areas that were constitutionally protected and locations that were not. Several decades later, after some significant erosion of that approach, the Court in *Katz v. United States*[29] explicitly rejected *Olmstead* and the concept of "constitutionally protected areas," stating that the Amendment protected people, not places. The Court ultimately adopted Justice Harlan's concurring view in *Katz*, establishing that the Amendment protects reasonable expectations of privacy. That test defines the *quality* protected — at least in part — but does not define what objects are protected. The reasonable expectation of privacy test generally has been used as an overlay to determine whether a person has a reasonable expectation of privacy — a protected interest — in the items listed in the Amendment. Hence, despite the sweeping possibilities implicit in *Katz*'s approach, the four items listed in the Amendment as the protected objects remain central to understanding the scope of what the Amendment protects. Indeed, in recent cases, the "constitutionally protected area" language and structure have reappeared.[30]

The protected interests analysis is structured as follows:

- Examination of the right to be "secure" includes:
  - overview of current analysis and historical meaning of word "secure" § 3.1.
  - origin, development, and [ostensible] demise of property analysis § 3.2.
  - expectations of privacy test, including hierarchy of privacy interests § 3.3.
  - measuring privacy expectations and techniques to create a hierarchy § 3.3.4.
  - critique of privacy as a centralizing principle § 3.3.5.
  - other protected interests, including liberty, property, the home, and possessory interests § 3.4.
  - a broader perspective of the right to be secure § 3.4.
- Several significant limitations on protected interests are discussed:
  - assumption of risk, voluntary exposure, and shared privacy § 3.5.1.
  - "standing" principles,[31] including procedural aspects of the standing question, current and rejected standing doctrines, and categories of persons seeking to challenge searches § 3.5.2.
- Overview of the characteristics of the four objects specifically mentioned in the Amendment:
  - "the people" § 4.2.
  - "persons" § 4.3.

---

27. *E.g.*, Oliver v. United States, 466 U.S. 170, 183–84 (1984) (holding that open fields are not protected by the Fourth Amendment); Hester v. United States, 265 U.S. 57, 59 (1924) (same).

28. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

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

30. *E.g.*, Florida v. Jardines, 569 U.S.___, 133 S. Ct. 1409 (2013); United States v. Jones, 132 S. Ct. 945 (2012); Kyllo v. United States, 533 U.S. 27 (2001).

31. In modern jurisprudence, standing is not an inquiry separate from the substantive question of what the Amendment protects. Despite the Court's treatment of standing as a substantive question, it operates in practice as an important limitation on the application of the exclusionary rule because only those persons who have a personal right affected by the search or seizure may challenge the admissibility of the evidence recovered. This is to say that standing doctrine has an important relationship to exclusionary rule policies.

- "houses," the curtilage doctrine, the open fields doctrine, and business and commercial premises, including closely regulated industries § 4.4.
- "papers" § 4.5.
- "effects," including abandoned property and garbage § 4.6.

§ 1.2.2. Satisfaction

§ 1.2.2.1. The reasonableness command

The first clause of the Fourth Amendment requires that a search or seizure not be "unreasonable." This is the "fundamental command"[32] of the Amendment and this "imprecise and flexible term" reflects the Framers' recognition "that searches and seizures were too valuable to law enforcement to prohibit them entirely" but that "they should be slowed down."[33] Reasonableness is the measure of both the permissibility of the initial decision to search and seize and the permissible scope of those intrusions.[34]

The wide scope of the Amendment's applicability continually creates new and unprecedented challenges to traditional notions of reasonableness. In the face of such challenges, the reasonableness analysis employed by the Supreme Court has repeatedly changed and each new case seems to modify the Court's view of what constitutes a reasonable search or seizure. For some time, the Court created substantive restrictions on the government's ability to search and seize, that is, there were categories of papers that could not be the target of a search or seizure. Those substantive restrictions were rejected in the latter part of the twentieth century and reasonableness is viewed as a procedural mechanism that regulates the circumstances when the government can intrude and the scope of that intrusion.

There are at least five principal models that the Court currently chooses from to measure reasonableness: the warrant preference model; the individualized suspicion model; the totality of the circumstances test; the balancing test; and a hybrid model giving dispositive weight to the common law. Because the Court has done little to establish a meaningful hierarchy among the models, the Court in any situation may choose whichever model it sees fit to apply. Thus, cases decided within weeks of each other have had fundamentally different — and irreconcilable — approaches to measuring the permissibility of an intrusion. The five main models and several situations that do not easily fit within any of those models are examined in Chapter 11. An alternative approach to measuring reasonableness is also proposed.

- The following aspects of the meaning of "unreasonable" are discussed:
  - importance of the concept of reasonableness § 11.1.
  - origins of the concept of reasonableness § 11.2.
  - procedural regulation of searches and seizures § 11.3.
  - model #1: the warrant requirement § 11.3.1.
  - model #2: individualized suspicion, including probable cause and articulable suspicion, and how individualized suspicion is obtained § 11.3.2.
  - model #3: case-by-case model § 11.3.3.
  - mode l#4: the balancing test, including its broad application § 11.3.4.

32. New Jersey v. T.L.O., 469 U.S. 325, 340 (1985).
33. Berger v. New York, 388 U.S. 41, 75 (1967) (Black, J., dissenting).
34. *E.g.*, New Jersey v. T.L.O., 469 U.S. 325, 341 (1985); Terry v. Ohio, 392 U.S. 1, 20 (1968).

- model #5: common law plus balancing § 11.3.5.
- situations that do not fit any of the five models, including bodily integrity, free speech and private conversation concerns, and the home § 11.3.6
- consent § 10.4.
- the Court's attempts to harmonize the various models § 11.4.
- proposed hierarchy of reasonableness § 11.5.

- Several other aspects of reasonableness are also considered:
  - scope of intrusion considerations, including least intrusive means analysis § 11.6.1.
  - pretextual actions, racial discrimination, and objective intent § 11.6.2.
  - bright line rules vs. case-by-case adjudication § 11.6.3.
  - unreasonable or excessive force § 11.6.4.

§ 1.2.2.2. Warrant issues, including issuance, review, and execution

The second clause of the Amendment sets forth the criteria for a warrant to issue: "and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Regardless of whether a warrant is *required* by a particular view of reasonableness, it is still the *preferred* manner of searching and seizing. Hence, the standards by which courts review a magistrate's decision to issue a warrant are quite deferential. The good faith doctrine has also significantly influenced this review. The Warrant Clause of Fourth Amendment regulates when a warrant may issue but says nothing about the execution of a warrant. Instead, warrant execution issues are regulated by the Reasonableness Clause.[35]

- Warrant issuance considerations discussed include:
  - overview of warrant issuance requirements §§ 12.1.–12.2.
  - review of the decision to issue a warrant, including probable cause deficiencies, attacks on the issuing magistrate, and misrepresentations by the affiant § 12.3.
  - particularity requirement of the Warrant Clause § 12.4.
- Warrant execution issues discussed include:
  - when an arrest or search warrant is needed to enter a home to arrest § 6.3.5.
  - time periods for warrants to be valid and staleness § 12.5.2.
  - nighttime execution of warrants § 12.5.3.
  - knock and announce requirements § 12.5.4.
  - return of warrants and inventory § 12.5.5.
  - executing warrants for intermingled documents/digital evidence § 12.5.6.
  - proper assistants — who may accompany the police § 12.5.7.

35. *E.g.*, United States v. Grubbs, 547 U.S. 90 (2006); Dalia v. United States, 441 U.S. 238 (1979). *See also* United States v. Banks, 540 U.S. 31 (2003) (stating that there is no "template" for when police must knock and announce before entering a house when executing a warrant and, in such cases, the "notion of [a] reasonable execution" of a warrant has to be "fleshed out" on a case-by-case basis). *But see* § 12.4.8. (discussing how some courts are using new warrant issuance requirements to regulate searches for digital evidence).

- searches of persons on premises when warrant executed § 12.5.8.
- detention of persons during the execution of a warrant § 6.7.
- use of force § 11.6.4.
- protective sweeps § 9.2.

§ 1.2.3. Remedies

The chief enforcement mechanism to ensure compliance with the Fourth Amendment is the exclusionary rule, which prohibits the introduction of illegally obtained evidence in the government's case-in-chief.[36] Although the rule was for some time considered constitutionally mandated, the Court now believes that the exclusionary sanction is a judicially created remedy designed to deter future police misconduct. It is not "'a personal constitutional right of the party aggrieved'" and it "is neither intended nor able to 'cure the invasion of the defendant's rights which he has already suffered.'"[37] Where appropriate, the remedy of exclusion extends to direct and indirect products of illegal intrusions, that is, "any 'fruits' of a constitutional violation — whether such evidence be tangible, physical material actually seized in an illegal search, items observed or words overheard in the course of the unlawful activity, confessions or statements of the accused obtained during an illegal arrest and detention,"[38] or testimony concerning knowledge acquired during an unlawful intrusion.[39]

An overriding consideration in contemporary exclusionary rule cases is the Court's use of a cost-benefit test to decide whether the rule ought to be applied. According to the Court, exclusion of evidence "exacts a costly toll upon the ability of courts to ascertain the truth in a criminal case"[40] and permits "some guilty defendants [to] go free or receive reduced sentences as a result of favorable plea bargains."[41] Thus, the Court has restricted application of the exclusionary rule to instances where its "remedial objectives are thought most efficaciously served."[42] Where the exclusionary rule does not result in appreciable deterrence of future police misconduct, the Court views its use as unwarranted.[43] Deterrence is now the rule's sole purpose, despite decades of Supreme Court declarations that that purpose has never been empirically proven and despite much skepticism about whether the rule does in fact deter.

The debate over application of the exclusionary rule often has been accompanied by references to the efficacy of alternative remedies, with a chief alternative being civil suits for damages. Other considerations include administrative sanctions against police officers and training programs to increase compliance with Fourth Amendment requirements. Traditionally, the Court has been skeptical about such alternatives — at least in the crim-

36. *E.g.*, Terry v. Ohio, 392 U.S. 1, 12–13 (1968).
37. United States v. Leon, 468 U.S. 897, 906 (1984).
38. United States v. Crews, 445 U.S. 463, 470 (1980).
39. *E.g.*, Murray v. United States, 487 U.S. 533, 536 (1988); Wong Sun v. United States, 371 U.S. 471 (1963).
40. United States v. Payner, 447 U.S. 727, 734 (1980).
41. United States v. Leon, 468 U.S. 897, 907 (1984).
42. United States v. Leon, 468 U.S. 897, 908 (1984) (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)).
43. Arizona v. Evans, 514 U.S. 1 (1995); United States v. Janis, 428 U.S. 433, 454 (1976).

inal trial context. More recently, however, a majority of the Court in *Hudson v. Michigan*[44] pointed to the availability of such alternatives and higher levels of police professionalism and training in the context of creating a *per se* exception to the exclusionary rule for knock and announce violations. The breadth of the majority's opinion put in doubt the continued existence of the exclusionary rule. Nonetheless, *Hudson* appears to be just another of a long line of inconsistent Supreme Court opinions. Indeed, the Court has candidly noted that the "debate" within the Court concerning the rule has always been a warm one and "the evolution of the exclusionary rule has been marked by sharp divisions in the Court."[45]

Shortly after *Hudson*, the Court's view took another apparent—and significant turn—in two cases, *Herring v. United States*[46] and *Davis v. United States*,[47] which appear to achieve most of the goals in *Hudson* by employing a more indirect approach: narrowing the rule to only situations where the police have engaged in demonstrably outrageous conduct. In *Herring*, and reaffirmed in *Davis*, the Court reframed the question as to whether the rule applied by focusing on the culpability of the police officer. If the broad language employed in those cases prevails, it will fundamentally change the litigation of motions to suppress in criminal cases. That is, a central question will be whether the officer had a culpable mental state; if not, the rule will not apply. If that mode of analysis prevails, it will reduce appreciably the number of cases addressing the merits of Fourth Amendment claims and expand dramatically the inapplicability of the exclusionary rule.

- Exclusionary rule issues discussed include:
  - evolution of exclusionary rule doctrine § 13.2.
  - fruit and attenuation analysis, including cost-benefit analysis § 13.3.
  - suppressing a defendant's statement, testimony of a witness, identification of the defendant, and the defendant's presence and physical characteristics § 13.3.
  - *per se* attenuation based on the interest protected: in-home arrests; knock and announce violations § 13.3.6.
  - independent source doctrine § 13.4.
  - inevitable discovery doctrine § 13.5.
  - good faith doctrine §§ 12.3., 12.4.9., 13.6.
  - impeachment § 13.7.
  - other remedies § 13.8.
  - standing § 3.5.2.

§ 1.3. Tools to interpret the Amendment

The Supreme Court has used a variety of interpretative tools as aids in formulating principles to implement Fourth Amendment commands. Depending on the era and whether a conservative or liberal majority holds sway on the Court, different tools have been utilized. Collectively, the cases are irreconcilable as to which tools are proper. To take just one example of the Court's inconsistencies, longstanding practices [48] (includ-

44. 547 U.S. 586 (2006).
45. United States v. Janis, 428 U.S. 433 (1976).
46. 555 U.S. 135 (2009).
47. 564 U.S. __ , 131 S. Ct. 2419 (2011).
48. Boyd v. United States, 116 U.S. 616, 622–23 (1886). The Court has often relied on the historical acceptance of the actions challenged to support its conclusion that the search or seizure without suspicion is reasonable. *See, e.g.*, United States v. Robinson, 414 U.S. 218, 230–35 (1973). *Cf.* Carroll v.

ing authorization by Congress[49] and particularly the first Congress[50]) have sometimes influenced the Court's decisions but at other times have not.[51]

The Court has repeatedly emphasized the need for a workable rule to guide the police officer on the street.[52] Thus, the Supreme Court has sometimes utilized bright-line rules[53] to guide the police in executing searches and seizures,[54] which do not require case-by-case justification and provide "clear legal boundaries to police conduct."[55] Yet, at other times, it has rejected such analysis, viewing bright lines as having utility only in exceptional situations[56] and maintaining that the limitations imposed by the Fourth Amendment must "be developed in the concrete factual circumstances of individual cases."[57] It almost never examines an officer's actual intent, preferring instead an objective[58] analysis of the facts presented, although it will at times examine programmatic purpose[59] and

---

United States, 267 U.S. 132, 149 (1925) ("The Fourth Amendment is to be construed in light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.").

49. Indeed, the Court has gone as far as to say that, when Congress has authorized a particular type of search, there is a "strong presumption" of constitutionality, "especially when it turns on what is 'reasonable.'" United States v. Di Re, 332 U.S. 581, 585 (1948). *Accord* United States v. Watson, 423 U.S. 411, 416 (1976).

50. *E.g.*, Boyd v. United States, 116 U.S. 616, 623 (1886). *Cf.* Carroll v. United States, 267 U.S. 132, 151 (1925) (examining actions of the first, second, fourth, and subsequent Congresses as evidence of reasonableness); Davis v. United States, 328 U.S. 582, 605–06 (1946) (Frankfurter, J., dissenting) (examining "contemporaneous" authorizations to search by the first Congress and by subsequent Congresses as demonstrating need for a warrant and illuminating intent to restrict ability to search unless authorized).

51. *E.g.*, Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) ("It is clear, of course, that no Act of Congress can authorize a violation of the Constitution."). *Cf.* Sibron v. New York, 392 U.S. 40, 59, 62 (1968) (refusing to determine whether the state statute that authorized the police procedure was constitutional and instead examining the actions of the officer to ascertain whether they comported with the Fourth Amendment's requirements).

52. *See, e.g.*, Illinois v. Andreas, 463 U.S. 765, 772 (1983); New York v. Belton, 453 U.S. 454, 459–60 (1981) ("When a person cannot know how a court will apply a settled principle to a recurring factual situation, that person cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority.").

53. *See* § 11.6.3.

54. *See, e.g.*, Maryland v. Wilson, 519 U.S. 408 (1997) (permitting police officers to order all passengers to exit a vehicle as an incident of a stop of any vehicle); New York v. Belton, 453 U.S. 454, 458 (1981) (A "'single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront.'") (quoting Dunaway v. New York, 442 U.S. 200, 213–14 (1979)).

55. David A. Harris, *Frisking Every Suspect: The Withering of* Terry, 28 U.C. Davis L. Rev. 1, 37 (1994). Such rules are premised on the recognition that the protections of the Fourth Amendment "'can only be realized if the police are acting under a set of rules which, in most instances, makes it possible to reach a correct determination beforehand as to whether an invasion of privacy is justified in the interest of law enforcement.'" New York v. Belton, 453 U.S. 454, 458 (1981) (quoting Wayne R. LaFave, "*Case-By-Case Adjudication" Versus "Standardized Procedures": The* Robinson *Dilemma*, 1974 S. Ct. Rev. 127, 142).

56. *E.g.*, Ohio v. Robinette, 519 U.S. 33, 39 (1996).

57. *E.g.*, Terry v. Ohio, 392 U.S. 1, 29 (1968). *Cf.* United States v. Rabinowitz, 339 U.S. 56 (1950), *overruled by* Chimel v. California, 395 U.S. 752 (1969):

> What is a reasonable search is not to be determined by any fixed formula. The Constitution does not define what are "unreasonable" searches and, regrettably, in our discipline we have no ready litmuspaper test. The recurring questions of the reasonableness of searches must find resolution in the facts and circumstances of each case.

58. *See* § 11.6.2.1.

59. *See* § 11.4.

express concerns about subterfuge.[60] That objective mode of analysis leaves challenges of racial discrimination to the Fourteenth Amendment.[61]

Historical analysis has long played a very important role in the Court's interpretation of the Fourth Amendment.[62] The historical abuses the Framers sought to prevent and the process by which the Amendment reached its final form have been a main interpretative tool in seeking to achieve an understanding of the Fourth Amendment. The historical record is complex, involving hundreds of years of evolution in the regulation of searches and seizures, with many contradictory developments. Rather than the broad currents of history, the events in England and in the American colonies during the period immediately preceding the American Revolution directly served as a catalyst for the Amendment's adoption; it is also the portion of the historical record that is most often recalled in Supreme Court opinions and by leading commentators in interpreting the Amendment.

There is a never ending debate whether the exact historical practices or broader values that are seen as underlying those practices are the important lessons of history. The common law at the time of the Framing of the Fourth Amendment has sometimes been viewed as dispositive.[63] In other cases, the Supreme Court has relied on the common law as a guide that influences how the Fourth Amendment is interpreted.[64] Using the common law as the measure of reasonableness is distinct from using the common law as the measure of the Framers' intent. As to the former, the common law rule as of 1791 *defines* what is reasonable. As to the latter, the common law is consulted to ascertain the Framers' intent, which is in turn used to justify reliance on some conception of reasonableness. Indeed, the historical *abuses* that prompted the Amendment were more important to the Framers than the common law search and seizure *requirements*, with the only notable exception being the common law search warrant, which served as the model for the Warrant Clause.[65] Hence, sometimes there is a broader recognition that the Amendment was designed by the Framers to protect individuals from unreasonable governmental intrusion.[66] Such a view maintains that the Framers intended not only to prohibit the specific

60. *See* § 10.8.

61. *See* § 11.6.2.2.

62. *See generally* Chapter 2. Also, the Court has utilized historical analysis to help define the specific terms of the Amendment, which is detailed throughout this treatise.

63. Wyoming v. Houghton, 526 U.S. 295 (1999). *See* § 11.3.5.

64. Exactly how that tool has been used, as with other interpretative techniques, varies with who wrote the opinion. *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 326 (2001) (Court is "guided" by common law in ascertaining meaning of reasonableness); Oliver v. United States, 466 U.S. 170, 183–84 (1984) (although "[t]he common law may guide consideration of what areas are protected by the Fourth Amendment," common law rights are not co-incident with the Fourth Amendment); Payton v. New York, 445 U.S. 573, 591 (1980) (common law view utilized to shed light on Framers' intent); Gerstein v. Pugh, 420 U.S. 103, 114 (1974) (common law acts as a guide to interpret Fourth Amendment). *See generally* David A. Sklansky, *The Fourth Amendment and the Common Law*, 100 Colum. L. Rev. 1739 (2000) (tracing Supreme Court treatment of the common law as an interpretative tool); Kathryn R. Urbonya, *Rhetorically Reasonable Police Practices: Viewing the Supreme Court's Multiple Discourse Paths*, 40 Am. Crim. L. Rev. 1387(2004) (observing that the Court's reasonableness "paradigm eventually led to Fourth Amendment doctrines that did not require officials to have suspicion of any wrongdoing").

65. *See, e.g.*, Davis v. United States, 328 U.S. 582, 597 (1946) (Frankfurter, J., dissenting) (Bill of Rights "reflects experience with police excesses"); Boyd v. United States, 116 U.S. 616, 626–27 (1886) (historical background was in "minds of those who framed the Fourth Amendment" as "explanatory of what was meant by unreasonable searches and seizures").

66. *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 9 (1977) ("What we do know is that the Framers were men who focused on the wrongs of that day but who intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth.");

evils of which they were aware, but also, based on the general terms they used, to give the Constitution enduring value beyond their own lifetimes.[67] In other words, according to that view, the chief interpretative tool is to be consistent with the Framers' values but not mired in the details of the search and seizure practices of 1791.

Occasionally, historical analysis has been rejected as a basis to interpret the Amendment.[68] The Court has occasionally asserted that law enforcement practices are not "frozen" by those in place at the time the Fourth Amendment was adopted.[69] Hence, the Court has sometimes asserted that interpretation of the Amendment evolves to permit modern developments.[70] Moreover, the Amendment applies to a wide array of governmental activity, not just law enforcement. Thus, the Court has at times maintained that the Amendment must be interpreted in light of contemporary norms and conditions.[71] This method of

---

United States v. United States Dist. Court, 407 U.S. 297, 313 (1972) ("Though the physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance."); Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971) ("If times have changed, reducing everyman's scope to do as he pleases in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important."); United States v. Lefkowitz, 285 U.S. 452, 467 (1932) (rejecting literal construction of words in favor of Amendment's purpose); Boyd v. United States, 116 U.S. 616 (1886) (Asserting that the Fourth Amendment should be interpreted liberally in favor of the security of the person, the Court stated: "It is the duty of courts to be watchful for the constitutional rights of the citizens and against any stealthy encroachments thereon."); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 353 (1974) ("The Bill of Rights in general and the Fourth Amendment in particular are profoundly anti-government documents."); Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 Stan. L. Rev. 555, 626–27 (1996) (arguing that the values underlying the Amendment, to protect individual rights, must be reflected in its application to modern conditions, where scientific invention has made it possible for government agents to violate privacy rights without employing physical power).

67. *See* John H. Ely, Democracy and Distrust: A Theory of Judicial Review 1–2 (1980) ("The Constitution proceeds by briefly indicating certain fundamental principles whose specific implications for each age must be determined in contemporary context.... That the complete inference will not be there—because the situation is not likely to have been foreseen—is generally common ground."); Joseph D. Grano, *Rethinking the Fourth Amendment Warrant Requirement*, 19 Am. Crim. L. Rev. 603, 620 (1982) ("The underlying grievances are certainly relevant to the interpretative task, but constitutional provisions cannot be properly viewed simply as shorthand statements for the specific grievances that gave rise to them."); James J. Tomkovicz, California v. Acevedo*: The Walls Close in on the Warrant Requirement*, 29 Am. Crim. L. Rev. 1103, 1137 (1992) ("Constitutional analysts generally agree that the document was meant to be more than a mere catalogue of forbidden actions." The Framers intended that the "underlying *values*" be honored.).

68. *See, e.g.*, Tennessee v. Garner, 471 U.S. 1, 12–15 (1985) (changing the common law rule permitting police to shoot at fleeing suspects in part because modern felonies differ significantly from common law felonies and because of technological changes in weaponry).

69. Steagald v. United States, 451 U.S. 204, 217 n.10 (1981); Payton v. New York, 445 U.S. 573, 591 n.33 (1980).

70. *Cf.* New Jersey v. T.L.O., 469 U.S. 325, 339 (1985) (In applying the Amendment to searches of school children by school authorities, the Court recognized that the government's interest included contemporary needs: "Maintaining order in the classroom has never been easy, but in recent years, school disorder has often taken particularly ugly forms: drug use and violent crime in the schools have become major social problems.").

71. *E.g.*, Payton v. New York, 445 U.S. 573, 600 (1980) (stating that "contemporary customs and norms necessarily play" a "large role" in assessing reasonableness); Steagald v. United States, 451 U.S. 204, 217 (1981) ("Crime has changed, as have the means of law enforcement, and it would therefore be naive to assume that those actions a constable could take in an English or American village three centuries ago should necessarily govern what we as a society, now regard as proper."); Tennessee v. Garner, 471 U.S. 1, 12–15 (1985) (changing the common law rule that had permitted the police to shoot at fleeing suspects in part because modern felonies differ significantly from common law felonies and

analysis is only inconsistent with the common law as a tool of interpretation if the latter is seen to have dispositive effect. The *lessons* of history are not inconsistent with the belief that the Constitution is a living document. Historical analysis is arguably important primarily to identify the values of the Framers, which should be used to inform the Court's adaptation of the Fourth Amendment to modern conditions.

Underlying many of the techniques to interpret the Amendment are two competing approaches: normative and empirical. One view is that rules must have a normative basis to avoid deprecation of Fourth Amendment protections by interpretation favoring governmental needs.[72] This approach is sometimes employed[73] but at other times the interpretative tools used are decidedly empirical in nature.[74] Given that the number and varieties of official intrusions into individuals' lives have increased exponentially as a result of the increasing complexities of society, the Court's willingness to use such an approach has often led to the conclusion that no protected individual interest has been invaded by the government.[75] An empirical approach, coupled with technological advances, serves to reduce a person's protected interests, inextricably leading to a smaller and smaller oasis of protection afforded by the Amendment.[76]

---

because of technological changes in weaponry). *But cf.* Richards v. Wisconsin, 520 U.S. 385, 392 n.4 (1997) (cautioning that "[i]t is always dangerous to ground exceptions to constitutional protections in the social norms of a given historical moment," given the Fourth Amendment's purpose of preserving that degree of privacy that was afforded at the time it was adopted).

72. The need for establishing normative-based principles to guide Fourth Amendment analysis is discussed by Professor Morgan Cloud in his article, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. Rev. 199 (1993). After analyzing the pragmatic basis that had come to dominate the Court's opinions in the latter part of the twentieth century, he concludes: "The Court's opinions demonstrate that if the fourth amendment is to function as a device that protects individual autonomy by limiting government power, its interpretation must rest upon a theory that emphasizes strong rules, yet is sufficiently flexible to cope with the diverse problems arising under the fourth amendment." He then argues for a rule-based interpretive theory of the Amendment, with the rules derived "from normative claims justified by the history and text of the amendment, but ultimately grounded in a value-based claim about the nature of the amendment." The fundamental principle he perceives is that the Fourth Amendment exists to enhance individual liberty by containing government power. He then claims: "Simply put, if liberty is the goal, rules are needed." He ultimately concludes that "the fourth amendment example teaches us that without some coherent system of rules designed to limit [the power of the government], solitary individuals who claim the right to be free from government intrusions will lose, and the principle of liberty embodied in the amendment gradually will disappear."

73. *E.g.*, Payton v. New York, 445 U.S. 573, 602 (1980) (rejecting inquiry into practical consequences of rule requiring warrant for in-home arrests because, *inter alia*, "such arguments must give way to a constitutional command that we consider to be unequivocal").

74. *See* § 3.3.

75. *See* § 3.3.3.1.

76. Rarely has the Court acknowledged the possibility of a normative approach when discussing the reasonable expectations of privacy standard. In *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979), the majority opined:

> Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment pro-

Perhaps, in the end, the choices the Court must make come down to two: is the Amendment designed to regulate law enforcement practices or is it designed to protect individuals from overreaching governmental intrusions?[77] The first choice is reflected in *California v. Hodari D.*,[78] where the Court sought to establish the point at which a seizure of a person occurred. The Court did not construe the word literally but chose instead the common law definition of an arrest to measure when a seizure has occurred; that definition requires physical touching or submission. Explaining its reasoning, the *Hodari D.* majority candidly stated: "We do not think it desirable, even as a policy matter, to stretch the Fourth Amendment beyond its words and beyond the meaning of arrest.... Street pursuits always place the public at some risk, and compliance with police orders to stop should therefore be encouraged." Justifying its position, the *Hodari D.* majority added:

> Only a few of those orders, we presume, will be without adequate basis, and since the addressee has no ready means of identifying the deficient ones it almost invariably is the responsible course to comply. Unlawful orders will not be deterred, moreover, by sanctioning through the exclusionary rule those of them that are *not* obeyed. Since policemen do not command "Stop!" expecting to be ignored, or give chase hoping to be outrun, it fully suffices to apply the deterrent to their genuine, successful seizures.

The second view is illustrated by *Boyd v. United States*.[79] In discussing why it construed the concept of a search and seizure broadly, that majority opined:

> Though the proceeding in question is divested of many of the aggravating incidents of actual search and seizure, yet ... it contains their substance and essence,

---

tection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

A persistent minority view on the Court has advocated a normative approach and maintained that, even if the actions could be observed, a reasonable expectation of privacy should be found based on standards used to measure legitimacy. *E.g.*, Florida v. Riley, 488 U.S. 445, 456 (1989) (Brennan, J., dissenting) (arguing that any conclusion that a reasonable expectation of privacy exists ultimately depends on the judgment "whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society"); California v. Greenwood, 486 U.S. 35, 53–54 (1988) (Brennan, J., dissenting) (arguing that the police are required to "adhere to norms of privacy that members of the public plainly acknowledge," and concluding that a person has a reasonable expectation of privacy in trash left for collection); California v. Ciraolo, 476 U.S. 207, 220 n.5 (1986) (Powell, J., dissenting) (Such standards include real property law, personal property law, and "'understandings that are recognized or permitted in society'" and the inquiry "necessarily focuses on personal interests in privacy and liberty recognized by a free society."); Dow Chem. Co. v. United States, 476 U.S. 227, 248–49 (1986) (Powell, J., concurring in part and dissenting in part) (using trade secret laws to justify the conclusion that an expectation of privacy was reasonable). *Cf.* Jerome Atrens, *A Comparison of Canadian and American Constitutional Law Relating to Search and Seizure*, 1 Sw. J.L. & Trade Am. 29, 34–35 (1994) (contrasting empirical approach of United States Supreme Court in measuring reasonable expectations of privacy with normative approach of Canadian Supreme Court); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 Ind. L.J. 549, 564 (1990) (arguing that the Court has turned the principle of knowing exposure to the public into a simple assumption-of-risk test, stripping the individual of a "great measure of fourth amendment protection" due to "living in a high-tech society," and thereby stripping the Fourth Amendment of its "normative values").

77. Chief Justice Rehnquist, during his long tenure at the Supreme Court, was a main proponent of the first view and his views significantly influenced Fourth Amendment analysis. *See generally* Symposium, *William Rehnquist's Fourth Amendment*, 82 Miss. L.J. 259 (2013).

78. 499 U.S. 621 (1991), discussed in Chapter 5.

79. 116 U.S. 616 (1886).

> and effects their substantial purpose. It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance. It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon. Their motto should be *obsta principiis*. ["withstand beginnings"]

§ 1.4. Independent state grounds

State courts have increasingly turned to analysis of their own search and seizure provisions to afford broader protections to individuals than the Fourth Amendment offers.[80] This treatise is about the Fourth Amendment. Although it at times points to significant departures from Fourth Amendment analysis by state courts, it is not designed to serve as a guide to state constitutional law.[81]

State search and seizure provisions vary significantly.[82] There are some unique textual differences, particularly among the original thirteen colonies, although many of the more modern search and seizure provisions are remarkably similar to the Fourth Amendment. With few exceptions, state appellate courts did not develop a significant body of search and seizure jurisprudence prior to 1961. In that year, by mandating that the federal exclusionary rule was applicable to the states, *Mapp v. Ohio*[83] largely federalized search and seizure jurisprudence. To that end, for the better part of a decade, the Warren Court dramatically altered Fourth Amendment principles. It changed, for example, the nature of

---

80. States can afford more protection to individuals than the Fourth Amendment does but if the state constitution is construed to offer less, the Fourth Amendment serves as a floor. *E.g.*, Arkansas v. Sullivan, 532 U.S. 769 (2001); Cooper v. California, 386 U.S. 58 (1967). Hence, for state judges, the question is whether the state constitution should be construed to afford more protection to individuals than the Fourth Amendment.

81. For commentary on this question, *see generally* Symposium, *Independent State Grounds: Should State Courts Depart from the Fourth Amendment in Construing Their Own Constitutions, and if so, on What Basis Beyond Simple Disagreement with the U.S. Supreme Court's Result?*, 77 Miss. L.J. 1 (2007). The symposium featured the following articles: Jack Landau, *Should State Courts Depart from the Fourth Amendment? Search and Seizure, State Constitutions, and the Oregon Experience*; Joseph Grasso, *"John Adams Made Me Do It": Judicial Federalism, Judicial Chauvinism and Article 14 of Massachusetts' Declaration of Rights*; Michael E. Keasler, *The Texas Experience: A Case for the Lockstep Approach*; Irma Raker, *Fourth Amendment and Independent State Grounds*; Thomas Davies, *Correcting Search-and-Seizure History: Now-Forgotten Common-law Warrantless Arrest Standards and the Original Understanding of "Due Process of Law"*; Robert Williams, *State Constitutional Methodology in Search and Seizure Cases*; Lawrence Friedman, *Reactive & Incompletely Theorized State Constitutional Decision-Making*.

82. The provisions are ably analyzed in Michael Gorman, *Survey: State Search and Seizure Analogs*, 77 Miss. L.J. 417 (2007); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

83. 367 U.S. 643 (1961).

the protected interest from property to privacy,[84] expanding coverage of the Amendment (ranging from administrative inspections[85] to many everyday street encounters[86]), imposing new standards by which to measure reasonableness,[87] and articulating a broadly applicable exclusionary rule,[88] with the apparent ability of defendants to vicariously assert the rights of others.[89] The Burger and the Rehnquist Courts modified and cut back on much of the Warren Court's search and seizure jurisprudence by restricting the concepts of a search[90] and a seizure,[91] de-constitutionalizing[92] and restricting the application of the exclusionary rule,[93] and adapting the Warren Court's reasonableness standards to be very government friendly.[94]

In 1977, Justice Brennan, a chief architect of the Warren Court's search and seizure jurisprudence, urged state courts to turn to their own constitutions to avoid the impact of the conservative counter-revolution.[95] That call has been heeded to some extent but, frankly, much of the state court analysis often appears to be little more than adopting a dissenting view from a United States Supreme Court case or maintaining a Warren Court analysis in lieu of a more current high Court precedent.[96] Prior to *Mapp*, few state law-based search and seizure principles were being generated that favored individual rights. Thus, to depart from federal precedent in this era, state courts are not returning to a golden age of protecting individual rights under their own constitutions. They are, instead, often reacting to a perceived change in federal interpretation that is less favorable to individuals than had been apparent in Warren Court opinions. On the other hand, a vibrant and principled development of search and seizure principles by state courts, unshackled by current Supreme Court doctrine, may ultimately influence the high Court's development of Fourth Amendment principles. Justice Souter, while serving on the Supreme Court of New Hampshire, aptly described the dilemma facing state courts: "If we place too much reliance on federal precedent we will render the State rules a mere row of shadows; if we place too little, we will render State practice incoherent."[97]

---

84. Katz v. United States, 389 U.S. 347 (1967).
85. *E.g.*, Camara v. Municipal Court, 387 U.S. 523 (1967).
86. Terry v. Ohio, 392 U.S. 1 (1968).
87. *E.g.*, Camara v. Municipal Court, 387 U.S. 523 (1967).
88. *E.g.*, Mapp v. Ohio, 367 U.S. 643 (1961).
89. *E.g.*, Jones v. United States, 362 U.S. 257 (1960), *overruled by* United States v. Salvucci, 448 U.S. 83 (1980).
90. *E.g.*, United States v. Place, 462 U.S. 696 (1983) (excluding dog sniffs from the definition of a search); United States v. Jacobsen, 466 U.S. 109 (1984) (excluding chemical testing of substance for presence of illegal drugs from definition of a search).
91. *E.g.*, California v. Hodari D., 499 U.S. 621 (1991).
92. United States v. Calandra, 414 U.S. 338 (1974).
93. *E.g.*, Rakas v. Illinois, 439 U.S. 128 (1978).
94. *See generally* § 11.3.4.
95. William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 Harv. L. Rev. 489 (1977).
96. For example, a large number of state courts reject the Supreme Court's definition of a seizure in *California v. Hodari D.*, 499 U.S. 621 (1991), on state constitutional grounds. *See* § 5.1.4.2.5. Indeed, the Court's decision in *Hodari D.* may be the single most important event persuading state courts to depart from Supreme Court opinions in construing their own constitutions. Yet, the reasoning of the courts rejecting *Hodari D.* generally have not broken new ground but have instead simply expressed a preference for pre-*Hodari D.* case law as a more proper measure of when a seizure occurs. The courts typically rely on the dissent in *Hodari D.* and the case law preceding that decision.
97. State v. Bradberry, 522 A.2d 1380, 1389 (N.H. 1986) (Souter, J., concurring specially).

§ 1.5. Acquiring digital evidence (computer searches)

This section offers an overview of the Fourth Amendment's role in the acquisition of digital evidence and an introduction to statutory regulation.[98] It takes no special insight to observe that digital evidence is everywhere and that law enforcement has learned its value. The Fourth Amendment regulates the acquisition of data stored on computers and other digital devices. What is less clear is the scope of its application to the acquisition of data in networks or in transit. Government acquisition of that data is at least partially regulated by statutes and the statutory requirements are generally more stringent than what the Fourth Amendment has been construed to require, resulting in statutory analysis often superceding Fourth Amendment analysis.

Many investigations involve a combination of both regulatory regimes. Hence, it is not uncommon for information about criminal activity to be brought to law enforcement's attention based on some Internet activity. For example, that activity could be in the form of an email, a conversation in a chat room, or an intrusion into a company's network. Law enforcement must utilize the statutory framework to trace the source of the activity and then operate within the Fourth Amendment framework to seize evidence on the digital device that was the source of the activity.[99] Some aspects of an investigation do not implicate any regulatory regime and law enforcement may, just like any private citizen, utilize the numerous ways that the Internet now offers to learn something to facilitate the investigation. For example, search engines such as Google, public web sites, and chat rooms offer access to a host of information to anyone who chooses to use them.

Almost 70 percent of all reported appellate decisions involving the search or seizure of digital evidence have been concerned with the recovery of child pornography.[100] The alcohol prohibition era had a significant influence on Fourth Amendment analysis in the 1920s and 1930s. The drug wars of the last 50 years have also impacted the structure of search and seizure jurisprudence. Now, during the digital age, governmental investigations designed to locate child pornography may soon have a similar influence.

Utilizing the structure presented in this Chapter and throughout this treatise, in analyzing any case involving digital evidence, it must be determined if the Fourth Amendment is applicable. The applicability question, in turn, is a two-sided inquiry: (a) does the governmental activity — which must be either a search or a seizure — invade (b) an individual interest protected by the Amendment? If the Amendment does not apply, that ends the inquiry; it does not matter if the governmental actions are reasonable or not. If the Amendment does apply, is it satisfied?

Regarding the applicability question, a fundamental question for data searches is where the data is located. A person seeking to challenge the propriety of a governmental search must establish that the individual has a protected interest, which the Supreme Court typically measures by ascertaining whether the individual has a legitimate expectation of pri-

98. *See also* Thomas K. Clancy, Cyber Crime and Digital Evidence — Materials and Cases (2011); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193 (2005).

99. *E.g.*, United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008).

100. *E.g.*, Thomas K. Clancy, *Digital Child Pornography and the Fourth Amendment*, 49 The Judge's Journal 26 (Judicial Division of the American Bar Association) (2010).

vacy that has been invaded by the government.[101] This expectation of privacy inquiry is two pronged; the individual must have a subjective expectation of privacy and that subjective expectation of privacy must be one that society is prepared to recognize as reasonable.[102] If either prong is missing, no protected interest is established.[103] The application of this doctrine to digital searches and seizures is not without critics;[104] nonetheless, it remains the framework to assess a person's ability to challenge the propriety of governmental searches.

It is important to distinguish between the exterior of the computer (including what is visible on the monitor's screen) and its contents. As to locating a computer, the person seeking to challenge plain view observations made upon observing the computer must establish an expectation of privacy in the place where the computer is stored.[105] Thus, for example, when computers are located in a common area accessible to other employees or members of the public, a person does not have a reasonable expectation of privacy as to observations of the physical components of that computer.[106] In contrast, homeowners have a reasonable expectation of privacy in their belongings, including computers, in their home.[107] Equally true, however, is the principle that persons with no expectation of privacy in someone else's home or that home's contents cannot challenge observation of, or the search or seizure of, another's computer in that home.[108]

Employees may have a legitimate expectation of privacy in the data on digital devices that have been given to them by their employers.[109] However, office policies, practices, or regulations influence that expectation of privacy.[110] To date, the Supreme Court has provided little guidance and lower courts have been applying the expectations of privacy framework.

The Fourth Amendment's role in the acquisition of data stored on computers and other digital devices that are owned or used by individuals must be distinguished from its role in the acquisition of data in networks, in transit, or recovered from a third party. The fundamental consideration, utilizing the current framework, is whether a person has a reasonable expectation of privacy in the data sought. There are several variables that need to be considered, including:

---

101. *See* § 3.3.

102. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979). *See also* United States v. Caymen, 404 F.3d 1196, 1200–01 (9th Cir. 2005) (no reasonable expectation of privacy in the contents of computers the person has stolen or obtained by fraud).

103. *See* § 3.3.3.

104. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (questioning the third party doctrine's application to "the digital age" as "ill suited" because "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical "place" and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis. So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology."); § 3.3.

105. *See, e.g.*, United States v. Poulsen, 41 F.3d 1330, 1334–37 (9th Cir. 1994) (person who failed to pay rent had no reasonable expectation of privacy in the contents of storage locker, including computer tapes).

106. *E.g.*, United States v. Nettles, 175 F. Supp. 2d 1089, 1093–94 (N.D. Ill. 2001).

107. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001). *See also* People v. O'Brien, 769 N.Y.S.2d 654, 656 (N.Y.A.D. 2003) (defendant had reasonable expectation of privacy in computer in his bedroom).

108. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

109. *E.g.*, City of Ontario v. Quon, 560 U.S. __, 130 S. Ct. 2619 (2010).

110. *See* § 3.5.1.1.

- What steps the person has taken to protect his or her privacy;
- What type of data is being sought; and
- Whether the data is obtained from a third party.

Due to the nature of the Internet, networks, and the manner in which communications occur, courts often find an absence of a reasonable expectation of privacy in the data or communication recovered by the government. Thus, for example, one does not have a reasonable expectation of privacy in public chat rooms on the Internet[111] or in files the individual offers to share in peer-to-peer networks.[112]

Another consideration is the type of information obtained. The Supreme Court has long distinguished between the content and noncontent aspects of communications. In *Smith v. Maryland*,[113] for example, the Court concluded that the Amendment did not regulate the capture of the numbers dialed from a telephone, distinguishing between the content of a communication and noncontent aspects of the communication. That "distinction remains important in the constitutional and statutory law governing the inspection of private communications, even as new technologies have dramatically altered the nature of communication itself."[114]

> For over one hundred years, the Supreme Court has held that the Fourth Amendment protects mailed letters and packages from inspection by postal authorities or other government agents. Yet from the start, the Court has distinguished between the content of a letter and the noncontent information disclosed on its envelope. Whereas noncontent envelope information is exposed and can be examined by anyone, the content of a letter is "as fully guarded from examination

111. *See* Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (no expectation of privacy in material posted on bulletin board system that had disclaimer that personal communications were not private); People v. Gariano, 852 N.E.2d 344 (Ill. Ct. App. 2006) (public chatroom); State v. Evers, 815 A.2d 432, 439–40 (N.J. 2003) (person had no reasonable expectation of privacy in "pornographic material he unloosed into the electronic stream of commerce when he e-mailed two photographs … to fifty-one chat-room subscribers"). As one court has stated: "Clearly, when Defendant engaged in chat room conversations, he ran the risk of speaking with an undercover agent." United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997).

112. Such programs are widely used for a variety of illegal activities, including copyright violations involving movies and music. It is a primary distribution scheme for child pornographers. A person seeking to trade files can download software that permits him to configure his computer to join such networks and share files. Law enforcement is well aware of such networks and task forces and police departments engage in operations to identify persons utilizing peer-to-peer technology to trade illicit images. Government agents join such networks, search for files, and determine which constitute child pornography. Government agencies have software tools available to them that permit searches of large numbers of computers on a P2P network and have the ability to catch thousands of offenders. The techniques, used for years and continually becoming more sophisticated, are now widely exploited by authorities and large numbers of offenders are being identified as a result. Once a file is located, there are a few steps that must be taken to identify the computer that holds the file. *See, e.g.*, United States v. Craighead, 539 F.3d 1073 (9th Cir. 2008). Agents thereafter employ a warrant, consent, or (hopefully) otherwise seek to comply with Fourth Amendment satisfaction standards to search the suspect's computer. The case law is uniform that persons who put files in a folder to share that others can access on peer-to-peer networks do not have a reasonable expectation of privacy in such files. *E.g.*, United States v. Borowy, 595 F.3d 1045 (9th Cir. 2010). The same principles of voluntary exposure and assumption of risk have been applied to P2P activities on local networks. *See, e.g.*, United States v. King, 509 F.3d 1338 (11th Cir. 2007).

113. 442 U.S. 735 (1979).

114. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 William and Mary L. Rev. 2105 (2009).

> and inspection" as it would be if the party mailing the letter had retained it in his or her own home.[115]

A leading case illustrating the content/noncontent distinction is *United States v. Forrester*.[116] In that case, the authorities caused to have installed a pen register analogue known as a "mirror port" on Alba's account with PacBell Internet, which enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited, and the total volume of information sent to or from his account. The court concluded that this information was noncontent and not protected by the Fourth Amendment:

> We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the "switching equipment that processed those numbers," e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.
>
> Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/ from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a prerecorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.[n.6][117]

---

115. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 William and Mary L. Rev. 2105 (2009).

116. 512 F.3d 500 (9th Cir. 2008).

117. [n.6] Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the

> The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. E-mail, like physical mail, has an outside address "visible" to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.
>
> Finally, the pen register in *Smith* was able to disclose not only the phone numbers dialed but also the number of calls made. There is no difference of constitutional magnitude between this aspect of the pen register and the government's monitoring here of the total volume of data transmitted to or from Alba's account. Devices that obtain addressing information also inevitably reveal the amount of information coming and going, and do not thereby breach the line between mere addressing and more content-rich information.

The court therefore held that the computer surveillance techniques that Alba challenged were not Fourth Amendment searches but cautioned that "more intrusive techniques or techniques that reveal more content information" might produce a different result.

In the non-digital world, if a third party discloses information to the government that an individual has provided to that third party, the individual typically will not have an interest protected by the Fourth Amendment.[118] This is based on the Court's view that no Fourth Amendment protection exists where a wrongdoer has a misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.[119] Such a "risk," according to the Court, is "probably inherent in the conditions of human society."[120] This is consistent with the Supreme Court's view that voluntary exposure to the public eliminates Fourth Amendment protection.[121] The courts typically apply those principles regarding email or text messages obtained from the intended recipient.[122]

What remains is whether there should be a protected interest in the contents of information held or transmitted by third party providers of services. Numerous commentators have argued for Fourth Amendment protections extending to information held by

---

person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures URLs would also divulge the particular articles the person viewed.

118. *See, e.g.*, Miller v. United States, 425 U.S. 435, 443 (1976) (stating rule); United States v. Horowitz, 806 F.2d 1222, 1225–26 (4th Cir. 1986) (no reasonable expectation of privacy in computer data sold to and stored on another company's computer).

119. Hoffa v. United States, 385 U.S. 293, 302 (1966).

120. *Id.* at 303.

121. Katz v. United States, 389 U.S. 347, 351 (1967).

122. *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("an email message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received"); United States v. Maxwell, 45 M.J. 406, 418–19 (C.A.A.F. 1996) (no reasonable expectation of privacy in emails after being received by another person); State v. Hinton, 280 P.3d 476 (Wash. Ct. App. 2012) (no reasonable expectation of privacy in text message recovered from recipient's cell phone); Commonwealth v. Proetto, 771 A.2d 823 (Pa. Super. Ct. 2001) (email from recipient).

third parties,[123] although few courts have actually addressed the issue as to the contents[124] of communications.[125] There is an extraordinary amount of information held by third parties that can potentially be exploited by law enforcement.[126] Broadly speaking, there are two categories of substantive data that are of concern: the use of networks and the Internet to transmit information from one party to another, such as the body of an email; and the use of cloud-based services to store, share, or process data.[127]

---

123. *See, e.g.*, Patricia I. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1403–12 (2004) (arguing that there is a reasonable expectation of privacy in communications held by Internet service providers).

124. Noncontent is almost universally viewed as not protected. Numerous courts have held that there is no Fourth Amendment protection against the disclosure of subscriber information by Internet service providers. *See* United States v. Christie, 624 F.3d 558 (3rd Cir. 2010) (no reasonable expectation of privacy in subscriber information provided to internet service provider); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (noting that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person — the system operator"); United States v. Cox, 190 F. Supp. 2d 330 (N.D.N.Y. 2002) (no reasonable expectation in subscriber information provided to Internet service provider); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (same); United States v. Hambrick, 55 F. Supp. 2d 504, 507–09 (W.D. Va. 1999) (individual has no reasonable expectation of privacy in his name, address, social security number, credit card number, screen name, and proof of Internet connection obtained from Internet service provider); Hause v. Commonwealth, 83 S.W.3d 1, 10–12 (Ky. Ct. App. 2001) (no standing of subscriber to challenge warrant that obtained his name, address, and screen name from Internet service provider). *But see* State v. Reid, 945 A.2d 26 (N.J. 2008) (holding that citizens have a reasonable expectation of privacy, protected by Article I, Paragraph 7, of the New Jersey Constitution, in the subscriber information they provide to Internet service providers).

125. *See* § 3.5.1. Justice Sotomayor has questioned the third party doctrine's application to "the digital age," maintaining that it is "ill suited" because "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). *Compare* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (finding that subscriber did have reasonable expectation of privacy in copies of his emails recovered from his internet service provider) *and* State v. Hinton, 280 P.3d 476 (Wash. Ct. App. 2012) (asserting that text and email messages in transit are protected by the Fourth Amendment); State v. Clampitt, 364 S.W.3d 605 (Mo. Ct. App. 2012) (finding subscriber had reasonable expectation of privacy in text messages recovered from cell phone service provider) *with* Rehberg v. Paulk, 598 F.3d 1268 (11th Cir. 2010) (person has no reasonable expectation of privacy in emails stored with ISP), *vacated*, 611 F.3d 828 (11th Cir. 2010); United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (expressing doubt but declining to decide whether there was a reasonable expectation of privacy in email recovered from Internet service provider). *See also* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev. 507, 522–28 (2005) (discussing third party disclosure doctrine's application to email and proposing that the only third party who should be able to disclose it is the intended recipient, not couriers of information).

126. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1089–1101 (2002) (cataloguing this development).

127. Individuals and companies have the ability to store, access, and share large quantities of information with "Cloud computing." The term is a metaphor that The National Institute of Standards and Technology states is "on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

> Cloud service providers offer services beyond just storing and sharing data. They also offer database management and mining and web services, including processing complicated and large sets of data as well as managing and providing access to medical records. . . .
> Although sixty-nine percent of people using the Internet use at least one cloud-based computing service, many on these platforms are not aware if and/or when they are using a cloud service. Even if they are aware, it is likely that even less people are aware of where their data is being stored at any given time.

Peter Brown, *Who has Jurisdiction over the Clouds? A Look into Cloud Computing and the Jurisdictional Issues Surrounding the Use of its Shared Networks and Servers*, 1010 PLI/Pat 139 (Practicing Law Institute 2010).

Generally speaking, a person has a Fourth Amendment protected interest when one has taken steps to exclude:[128] close the door; close the drapes; seal the letter in an envelope; enter into a contract for a self storage locker or a safe deposit box. Thus, for example, Katz took steps to exclude the unwanted ear by closing the door to the telephone booth.[129] Renters have a protected interest in storage lockers.[130] The same should be true in the digital world: encrypt the body of the email; enter into a contractual relationship with a cloud computing service that offers privacy. The Internet is not structured to protect privacy; one must take steps to exclude. It is more like a shopping mall where there is no right to exclude (or have privacy). Indeed, unlike the relatively passive invitations to shop that stores offer in a mall, Internet service providers and websites are designed to obtain information about those using the services and to exploit that information. Like Katz, those seeking to prevent prying must take steps to do so. An encrypted email message is the same as a letter in a sealed envelope;[131] surely the government could open that flimsy white envelope and it may now have the capacity to decrypt the email message. But in both situations, the person has taken steps that, normatively, society acknowledges as reasonable (to use privacy analysis) and to exclude (to use security analysis).[132] An unencrypted email is not like a letter—its like a post card. There are now a variety of web-based services that offer remote storage and computing. These, in my view, are akin to a self-storage unit; the parties enter into a contract that, normatively, gives the individual a protected interest.[133]

Turning to Fourth Amendment satisfaction, the Supreme Court has provided virtually no guidance and there is a fundamental split in the lower courts on how to treat the acquisition of digital evidence. There are two principal approaches, which are discussed in section 12.4.8. One view asserts that a computer—or any digital device—is a form of a container and that the data in electronic storage in that device are mere forms of documents. Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers. Perhaps the most significant consequence

128. *See* § 3.4.4.

129. *See* Katz v. United States, 389 U.S. 347, 351–52 (1967) (Amendment protects information that a person "seeks to preserve as private").

130. United States v. Karo, 468 U.S. 705, 720 n.6 (1984).

131. *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages … are as fully guarded against examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."). *Jackson* distinguished letters from mail open to inspection, such as newspapers and magazines. *Id*.

132. *Cf.* United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008) (person posting files in folder on his computer to share on peer-to-peer network has no legitimate expectation of privacy and "is like saying that he does not know enough to close his drapes.").

133. The contract framework does not work for email. There are a variety of service agreements and some are protective of privacy and some are not. *Compare* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (finding expectation of privacy in emails obtained from ISP) *with* United States v. Warshak, 532 F.3d 521 (6th Cir. 2008) (en banc) (cataloging varieties of ISP agreements and using a contract analysis to opine that a legitimate expectation of privacy varied with the terms of the agreement). More fundamentally, however, once one sends an email, it passes through many service providers, most of which are not bound by the contractual agreement that one has with the person's Internet service provider. Hence, if an email is sent by X using ISP#1 to Y, who has a contract with ISP#2, ISP#2 is in no way bound by X's agreement with ISP#1. The government could acquire the email from ISP#2 without implicating X's contractual rights. If X encrypts the email, that manifestation of the intent to exclude applies to all intermediaries. Of course, the recipient who decrypts the email could still give it to the government.

of that view results from the application of the plain view doctrine: in any legitimate search that permits looking at digital data, potentially all data can be examined to ascertain what it is. A second view maintains that searches for data require a "special approach."[134] This view supports creating unique procedures and detailed justifications for warrants to issue,[135] new limitations on the permissible scope of intrusions,[136] and new rules for search execution procedures.[137] Underlying that approach, in large part, is a concern for broad searches akin to general searches. Notably, some courts see the new rules as having a limited shelf life:

> We realize that judicial decisions regarding the application of the Fourth Amendment to computer-related searches may be of limited longevity. Technology is rapidly evolving and the concept of what is reasonable for Fourth Amendment purposes will likewise have to evolve.... New technology may become readily accessible, for example, to enable more efficient or pinpointed searches of computer data, or to facilitate onsite searches. If so, we may be called upon to reexamine the technological rationales that underpin our Fourth Amendment jurisprudence in this technology-sensitive area of the law.[138]

Broadly generalizing, statutory requirements for government acquisition of data on the Internet and in networks tend to be more stringent than what the Fourth Amendment has been construed to require. In contrast to the Fourth Amendment, the Electronic Communications Privacy Act (ECPA) provides a more developed framework to regulate government interception of some—but not all—Internet communications.[139] The three relevant portions of ECPA are:

- The Wiretap Act,[140] which governs interception of the contents of communications in real time.
- The Pen Registers and Trap and Trace Devices statute,[141] which governs interception of the noncontent aspects of communications in real time.
- The Stored Communications Act,[142] which regulates access to the content and noncontent of records held in electronic storage by certain entities.

These statutes are in large part a reaction to Supreme Court decisions interpreting the Fourth Amendment and are, broadly speaking, designed to provide more protections to

134. This was the characterization of the court in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).
135. *See* § 12.4.8.2.2.
136. *See* § 12.4.8.2.2.
137. *See* § 12.5.6.
138. United States v. Hill, 459 F.3d 966 (9th Cir. 2006).
139. For a good overview of ECPA, *see* Charles Doyle, Privacy: An Overview of The Electronic Communications Privacy Act (Congressional Research Service, Oct. 2012).
140. 18 U.S.C. §§ 2510-22.
141. 18 U.S.C. §§ 3121-27.
142. 18 U.S.C. §§ 2701-11.

individuals. In *Olmstead v. United States*,[143] the Court held that the Amendment did not regulate wiretapping but observed that Congress had the power to do so if it so chose. Congress responded by enacting the predecessor of the current statute that regulates wiretapping of phone calls; after numerous revisions,[144] the Wiretap Act now covers the interception of oral, electronic, and wire communications, including Internet communications. In *Smith v. Maryland*,[145] the Court concluded that the Amendment did not regulate the capture of the numbers dialed from a telephone, distinguishing between the content of a communication and non-content aspects of the communication. In reaction, the predecessor of the current version of the Pen Register statute, which governs the interception of the noncontent aspects of communications in real time, was passed in 1986 as part of the broader Electronic Communications Privacy Act. Under ECPA, two important statutory considerations are whether the government is seeking the contents of the communication or merely noncontent; and whether the interception occurs as the communication occurs ("real time" interception) or whether the communication is in electronic storage.[146]

Each of these acts have evolved over time and they have generated much litigation. The reach and importance of each statute is subject to debate. Indeed, one court has observed that the intersection of the wiretap and stored communications acts "is a complex, often convoluted, area of the law."[147] That difficulty is "compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web."[148]

The distinction between content and noncontent information is critical in determining the level of statutory protection. ECPA offers much less protection to noncontent information than content information. The Wiretap Act governs the interception of communications content in transit and provides the most protection, including stringent requirements for a wiretap order to issue and a suppression remedy. The Pen Register Act governs the interception of the noncontent associated with communications; it requires a very low threshold to obtain an order and does not have an exclusionary remedy. The Stored Communications Act, which is the most complicated of the three statutes, regulates retrospective access to both the content and noncontent of communications held in electronic storage by certain communications providers. It offers different levels of protection through a hierarchical structure of types of process, depending on several contingencies, including the type of communications provider that has the information, the type of information sought, and how long the information has been in storage.

---

143. 277 U.S. 438 (1928), discussed in § 7.4.1.2.

144. A substantial revision occurred in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and often referred to thereafter as "Title III"); it was again updated by ECPA in 1986.

145. 442 U.S. 735 (1979), discussed in § 3.5.1.1.

146. In *Zurcher v. The Stanford Daily*, 436 U.S. 547 (1978), the Court refused to require authorities to first seek to obtain evidence held by a newspaper by means of a subpoena prior to resorting to a search warrant; the Court stated: "The Fourth Amendment has itself struck the balance between privacy and public need, and there is no occasion or justification for a court to revise the Amendment and strike a new balance by denying the search warrant in the circumstances present here and by insisting that the investigation proceed by subpoena *duces tecum*." The Privacy Protection Act, 42 § U.S.C. 2000aa, regulates government searches and seizures of material that agents have reason to believe may be related to First Amendment activities such as publishing or posting materials on the Internet.

147. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

148. Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002).

The Pen Register Act[149] was adopted in response to *Smith v. Maryland.*[150] *Smith* rejected the view that a person had any reasonable expectation of privacy in the numbers dialed from his telephone, thus permitting law enforcement agencies to obtain that dialing information without complying with the Fourth Amendment. A pen register records digits dialed on a telephone and a trap and trace device shows what numbers call a specific telephone, that is, all incoming phone numbers. The Pen Register Act initially applied to devices that recorded outgoing and incoming telephone numbers. Congress later amended the statutory definition of pen registers and trap and trace devices to include any "device or process" that records "dialing, routing, addressing, or signaling information," other than content information, associated with an electronic communication. It cannot be used to obtain the content of a communication.[151]

> A pen register and a trap and trace device may be a "process" used to gather information relating to "electronic communication." As for the term "electronic communication," the statute points to the definition found in 18 U.S.C. §2510. That statute defines the term "electronic communication" to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . ." 18 U.S.C. §2510(12). Given that the statute defines an electronic communication to be any "transfer of signals" of "any nature" by means of virtually any type of transmission system (*e.g.,* wire, electromagnetic, etc.), there can be no doubt it is broad enough to encompass e-mail communications and other similar signals transmitted over the Internet. It therefore follows that pen registers and trap and trace devices may be processes used to gather information about e-mail communications.
>
> There is some concern that current technology, particularly the use of a software process to obtain the requested information, increases the risk that content will be impermissibly procured and disclosed to the Government. A perhaps oversimplified response to that concern is that the stricture to avoid the contents of e-mail communications should be easy to comply with so long as the pen register and trap and trace processes or devices exclude all information relating to the subject line and body of the communication. The better approach, however, may be to take heed of the fact that "pen registers" and "trap and trace devices" are statutorily defined as processes or devices that are prohibited from collecting "the contents of any communication." 18 U.S.C. §3127(3)-(4). Consequently, the argument could be made that any process or device that collects the *content* of an electronic communication is not, in fact, a pen register or trap and trace device but, instead, is an electronic intercepting device as defined in Title III of the Omnibus Crime Control and Safe Streets Act, codified at 18 U.S.C. §§2510-2520.[152]

149. 18 U.S.C. §§3121-3127.

150. 442 U.S. 735 (1979).

151. "'Contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication." 18 U.S.C. §2510(8).

152. In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of A Pen Register and a Trap & Trace Device on E-Mail Account, 416 F. Supp. 2d 13 (D.D.C. 2006). *See also* In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (distinguishing between "post-cut-through dialed digits" ("PCTDD"), which are any numbers dialed from a telephone after the call is initially setup or 'cut-through'" and concluding that PCTDD

The statute expresses a general prohibition against the installation or use of a pen register without a court order.[153] A government attorney may apply for a court order authorizing installation of pen register and/or trap and trace device if "the information likely to be obtained is relevant to an ongoing criminal investigation."[154] The standard for obtaining a court order is far from burdensome. An attorney for the Government must make an application for authorization to install and use a pen register "in writing under oath or equivalent affirmation, to a court of competent jurisdiction."[155] Such an application need only contain:

> (1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and (2) certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.[156]

Upon a finding that this burden has been met, the court "shall enter" such an order.[157]

The Wiretap Act,[158] often referred to as "Title III," regulates the interception of the contents[159] of wire,[160] oral,[161] or electronic[162] communications, that is, "real time" capture of

---

contain the "contents of communication"); In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [Xxx] internet Service Account/user Name, 396 F. Supp. 2d 45 (D. Mass. 2005) (examining the complexity of "content" when applied to email and other activity on the Internet).

153. 18 U.S.C. § 3121(a).

154. 18 U.S.C. § 3122(b)(2).

155. 18 U.S.C. § 3122(a)(1).

156. 18 U.S.C. § 3122(b).

157. In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices, 515 F. Supp. 2d 325 (E.D.N.Y. 2007). *See also* In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of A Pen Register and a Trap & Trace Device on E-Mail Account, 416 F. Supp. 2d 13 (D.D.C. 2006) ("So long as an attorney for the Government applies for a 'pen register' or 'trap and trace device' and the court finds that the attorney certified that the information obtained using the devices is relevant to an ongoing criminal investigation, the court is mandated to enter an *ex parte* order authorizing the use of the devices.").

158. 18 U.S.C. §§ 2510-22.

159. "Content" is "information concerning [its] substance, purport, or meaning." 18 U.S.C. § 2510(8). *See, e.g.*, *In re* iPhone Application Litigation, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012), where the court observed:

> In *United States v. Reed*, 575 F.3d 900 (9th Cir. 2009), the Ninth Circuit held that data automatically generated about a telephone call, such as the call's time of origination and its duration, do not constitute 'content' for purposes of the Wiretap Act's sealing provisions because such data 'contains no "information concerning the substance, purport, or meaning of [the] communication."' *Id.* at 916 (quoting 18 U.S.C. 2510[(8)]). Rather, 'content' is limited to information the user intended to communicate, such as the words spoken in a phone call. *Id.* Here, the allegedly intercepted electronic communications are simply users' geolocation data. This data is generated automatically, rather than through the intent of the user, and therefore does not constitute 'content' susceptible to interception.

160. "Wire communication," is defined in § 2510(1): "any aural transfer … of communications by … aid of wire, cable, or other like connection … furnished or operated … for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." "Aural transfer" § 2510(18) is defined as any communication "containing the human voice at any point." Although the definition of a wire communication is complex, the most important aspect is that the communication must include the human voice. For example, all voice telephone communications qualify as wire communications.

161. "Oral communication" is defined in § 2510(2): "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."

the communications in transit.[163] The statute only applies to the interception of the contents of a communication.[164] The Act has been described as "complex" and "famous (if not infamous) for its lack of clarity."[165] The iconic example of the application of the Act is wiretapping a person's phone but it now applies to many other modes of communication.

Subject to exceptions, the statute sets out a general rule: it prohibits using an electronic, mechanical, or other device to intercept the contents of private wire, oral, or electronic communications between parties.[166] The prohibition applies to everyone in the United States, including private parties and governmental entities. The statute requires interception of a covered communication.[167] Although the statute does not explicitly require that the interception be contemporaneous with the transmission of the communication, "a contemporaneous requirement is necessary to maintain the proper relationship" between the Wiretap Act and the Stored Communications Act.[168] Every Circuit that has considered the question has adopted that view.[169] Hence, a person who accesses a stored copy of a communication does not "intercept" that communication.[170] Thus, in *United States v. Steiger*,[171] the court observed that the effect of a contemporaneous requirement for an intercept means that very few seizures of electronic communications from computers will constitute "interceptions":

> [T]here is only a narrow window during which an E-mail interception may occur—the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an em-

---

162. "Electronic communication" is defined in § 2510(12):
> "any transfer of signs, signals, writing, images, sounds, data, or intelligence … by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but … not (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device …; or (D) electronic funds transfer information stored by a financial institution."

163. The original act only covered wire and oral communications but Congress amended it in 1986 to include electronic communications. *See, e.g.*, Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995). It now applies to most Internet communications, including the body of an email. In *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002), the court provided another example:
> Website owners … transmit electronic documents to servers, where the documents are stored. If a user wishes to view the website, the user requests that the server transmit a copy of the document to the user's computer. When the server sends the document to the user's computer for viewing, a transfer of information from the website owner to the user has occurred. Although the website owner's document does not go directly or immediately to the user, once a user accesses a website, information is transferred from the website owner to the user via one of the specified mediums. We therefore conclude that Konop's website fits the definition of "electronic communication."

164. "Contents" § 2510(8): "any information concerning the substance, purport, or meaning of that communication."

165. Steve Jackson Games v. United States Secret Service, 36 F.3d 457, 461 (5th Cir. 1994).

166. 18 U.S.C. § 2511(1)(a).

167. "Intercept" § 2510(4): "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

168. Computer Crime and Intellectual Property Section, U.S. Dept. Of justice, Prosecuting Computer Crimes 165 (2009).

169. *See, e.g.*, Fraser v. Nationwide Mutual Insurance, 352 F.3d 107, 113 (3rd Cir. 2004); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003).

170. *E.g.*, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460–63 (5th Cir. 1994).

171. 318 F.3d 1039 (11th Cir. 2003).

> ployee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

For example, in *Steiger*, a computer hacker trolling the Internet used a Trojan Horse to gain access to Steiger's computer. He found child pornography files. In rejecting the claim that the hacker violated the Wiretap Act, the court stated:

> There is nothing to suggest that any of the information provided in the [hacker's] e-mails to the [government agents] was obtained through contemporaneous acquisition of electronic communications while in flight. Rather, the evidence shows that the source used a Trojan Horse virus that enabled him to access and download information stored on Steiger's personal computer. This conduct, while possibly tortious, does not constitute an interception of electronic communications in violation of the Wiretap Act.

There is, however, some disagreement among courts as to whether a communication is intercepted if acquired while in transient electronic storage.[172]

Wiretap orders have more stringent requirements to issue than a traditional warrant. A court may grant a wiretap order for wire communications only to investigate specified predicate offenses or for electronic communications to investigate any federal felony.[173]

> A federal court may issue a Wiretap Order "if it determines, on the basis of the facts submitted by the applicant, that there is probable cause to believe (1) that an individual was committing, had committed, or is about to commit a crime; (2) that communications concerning that crime will be obtained through the wiretap; and (3) that the premises to be wiretapped were being used for criminal purposes or are about to be used or owned by the target of the wiretap." *United States v. Diaz*, 176 F.3d 52, 110 (2d Cir.1999) (citing 18 U.S.C. §2518(1)(b)(I), (3)(a), (b), (d)). The applicable standard for probable cause is the same as the standard for a search warrant, which is established if the "totality-of-the-circumstances" indicates a probability of criminal activity.[174]
>
> The government must prove necessity by making "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous…." §2518(1)(C)). The issuing judge may approve the wiretap if the judge determines that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous…." §2518(3)(C)). These requirements ensure that "wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime."[175]

Violations of the Wiretap statute may give rise to criminal liability,[176] and/or civil liability.[177] The statute authorizes a suppression remedy,[178] but, as a general rule, it is only

---

172. *See* United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (electronic communications can be intercepted even if they are in electronic storage so long as the communications are in transient electronic storage intrinsic to the communication process).

173. 18 U.S.C. §2518.

174. In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices , 515 F. Supp. 2d 325 (E.D.N.Y. 2007).

175. United States v. Reed, 575 F.3d 900 (9th Cir. 2009).

176. *See* 18 U.S.C. §2511(4).

177. *See id.* §2520.

178. *See id.* §2518(10)(a).

available for illegal wiretaps of *wire* or *oral* communications — not of *electronic* communications.[179] To obtain suppression, the person must have been a party to the wire or oral communication.[180] There are other important qualifications to the scope of the suppression remedy not discussed here.[181]

The Stored Communications Act[182] regulates access to and disclosure of stored electronic communications or account records held by network service providers such as Internet service providers. It has no applicability to data in real time transit. Whenever government investigators seek stored email, account records, or subscriber information from certain defined classes of service providers, they must comply with the SCA.[183] The Act serves several purposes: it creates criminal penalties for unauthorized access to certain stored communications; it creates a procedure for compelled disclosure of stored information to federal and state law enforcement officials; and it sets out the circumstances under which network service providers many voluntarily disclose information. It does not have a suppression remedy. The SCA sets out a series of classifications, reflecting the drafters' belief that different types of information are more or less deserving of privacy protection. It is a complex statute and courts have differed on the meaning of several of its provisions.

> When a person uses the Internet, the user's actions are no longer in his or her physical home; in fact he or she is not truly acting in private space at all. The user is generally accessing the Internet with a network account and computer storage owned by an [internet service provider] like Comcast or NetZero. All materials stored online, whether they are e-mails or remotely stored documents, are physically stored on servers owned by an ISP. When we send an e-mail or instant message from the comfort of our own homes to a friend across town the message travels from our computer to computers owned by a third party, the ISP, before being delivered to the intended recipient. Thus, "private" information is actually being held by third-party private companies.[184]

---

179. *See* United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003).

180. *See* 18 U.S.C. §2518(10)(a).

181. *See* Searching and Seizing Computers and Obtaining Electronic Evidence 183–88 (Computer Crime and Intellectual Property Section, U.S. Dept. of Justice 2009).

182. 18 U.S.C. §§2701-12.

183. Electronic storage is defined by the statute as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an [ECS] for purposes of backup protection of such communication." 18 U.S.C. §2510(17). Courts differ as to the meaning of this provision. The first category refers to temporary storage, such as when a message sits in an e-mail user's mailbox after transmission but before the user has retrieved the message from the mail server. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005). An email in post-transmission storage (*i.e.*, that has reached its intended destination) is no longer in "electronic storage" because the storage, whether on an end user's computer or as a copy left on a service provider's computer, is no longer "temporary" nor "incidental to … transmission." *See, e.g.*, Fraser v. Nationwide Mutual Insurance Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001), *aff'd in part*, 352 F.3d 107 (3rd Cir. 2003). Hence, the SCA does not apply to post-transmission storage of communications. Under this view, once the communication reaches its destination, it is no longer in "temporary, intermediate storage." There is another view that maintains that a message in post-transmission backup storage on the provider's system is still in "electronic storage." Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

184. In the Matter of the Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210 (D. Or. 2009).

The SCA applies only to two types of network service providers: providers of an "electronic communication service"[185] and providers of a "remote computing service."[186] If a provider does not fit within these definitions, the SCA does not regulate disclosures of information by that provider. Whether a provider is in either of those two classes or neither class depends on the nature of the particular communication sought. A provider can simultaneously provide "electronic communication service" with respect to one communication and "remote computing service" with respect to another communication, or a public provider can consecutively provide such services with respect to the same communication. Into which category a provider falls is fundamental in determining what the provider may disclose voluntarily and the type of process needed to compel disclosure.[187]

The statute sets out graduated requirements for the government to seek compelled access to information, depending on the type of information sought. In other words, the type of process needed varies with the type of information sought.[188] When providers are not allowed or do not choose to voluntarily disclose content or records, the government can compel providers to disclose information through appropriate legal process, depending on the nature of the communication storage. There are five different levels of process. The more "process" utilized yields more types of information.

> The standard for court orders differs according to the duration of electronic storage and whether the information obtained is content or noncontent. At the highest level, ordering an ISP to turn over the contents of electronic communications stored for 180 days or less requires a standard search warrant. Communications contents stored for more than 180 days can be obtained either with a standard warrant or a subpoena (or a §2703(d) court order) that must be coupled in most cases with prior notice to the ISP subscriber. A subscriber who has been notified that his personal information has been subpoenaed would likely have the op-

185. An "electronic communication service" under §2510(15) is defined as: "any service which provides … users … the ability to send or receive wire or electronic communications."

186. A "remote computing service" under §2711(2) is defined as: "the provision to the public of computer storage or processing services by means of an electronic communications system." The statute does not define "to the public" but the "word 'public,' however, is unambiguous. Public means the 'aggregate of the citizens' or 'everybody' or 'the people at large' or 'the community at large.' Thus, the statute covers any entity that provides electronic communication service (*e.g.*, e-mail) to the community at large." Andersen Consulting LLP v. UOP and Bickel & Brewer, 991 F. Supp. 1041 (N.D. Ill. 1998).

187. "The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question." Computer Crime and Intellectual Property Section, U.S. Dept. Of justice, Prosecuting Computer Crimes 120 (2009). "Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself. The distinction is still essential, however, because different services have different protections." In the Matter of the Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210 (D. Or. 2009).

188. Basic Subscriber and Session Information, under §2703(c)(2), consists of the following categories: name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number). Records or Other Information Pertaining to a Customer or Subscriber is defined in §2703(c)(1) as: "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." Finally, contents under §2510(8) means: "includes any information concerning the substance, purport, or meaning of that communication."

portunity to challenge the subpoena on the grounds of irrelevance, improper purpose, or procedural flaws. Numerous courts have recently held that a privacy interest inherent in many personal records (such as credit card or employment personnel records) allows the subject of the records to challenge subpoenas issued to third parties.

At the lowest level, only a subpoena is required to compel an ISP to disclose basic noncontent subscriber information, including name, address, records of session times, length and type of subscription, telephone number or network address, and source of payment including credit card number. A somewhat higher level of protection is granted to "other" noncontent records pertaining to the subscriber, a category that generally covers all transactional information (such as phone usage records or records of email headers) other than basic subscriber information. For these records, the government must generally obtain a § 2703(d) court order, which can be issued only if the government applicant provides "specific and articulable facts" demonstrating "reasonable grounds to believe that the [records] are relevant and material to an ongoing criminal investigation." Ironically, this standard is significantly higher than the standard governing Pen Register Act intercept orders, which generally provides no judicial review and requires no showing of specific and articulable facts. The "reasonable grounds for relevance" standard is lower than probable cause (and is akin to the general relevance standard for subpoenas), but does provide some degree of judicial scrutiny for noncontent record requests. Still, the standards for obtaining content in the ECPA, even content stored for more than 180 days, are substantially higher than those for noncontent. The lowest standard for obtaining stored content still requires notice to the subscriber (and the corresponding opportunity to challenge the surveillance); on the other hand, the highest standard for noncontent information does not require notice to the subscriber whose records are being observed. The statutory protection afforded to electronic communication information depends in large part on whether the information is classified as content or noncontent information under the ECPA.[189]

There have been few successful Fourth Amendment challenges to this framework. Notably, however, the Sixth Circuit, in two connected cases, has considered the question whether an order under section 2703(d) is sufficient to satisfy the Fourth Amendment when used to obtain the contents of a subscriber's email from an Internet Service Provider. In the first of two connected cases, when the subscriber sought injunctive relief to prevent the government from using that procedure in the future, the en banc court rejected the subscriber's claim as unripe; however, the court discussed in detail some of the variables that might affect the reasonableness of the subscriber's expectation of privacy in emails.[190] The subscriber, Steven Warshak, was convicted of a variety of federal crimes and, in a later decision, a panel of the court found that his Fourth Amendment rights had been violated when the contents of his emails were turned over to the authorities based on the § 2703(d) order.[191] Combining the statutory framework with cases such as *Warshak*,[192] the current status of protection for stored communications is very uncertain.

---

189. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 William & Mary L. Rev. 2105 (2009).

190. Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc).

191. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

192. *Cf.* Rehberg v. Paulk, 598 F.3d 1268 (11th Cir. 2010) (person has no reasonable expectation of privacy in emails stored with ISP), *vacated*, 611 F.3d 828 (11th Cir. 2010).

This treatise covers the following topics concerning the Fourth Amendment aspects of obtaining digital evidence:

- assumption of risk—expectations of privacy in work digital devices; joint users § 3.5.1.1.
- data as "papers" § 4.5.
- digital devices as containers § 4.6.1.
- seizures of digital evidence § 5.2.4.
- plain view doctrine's application to computer screens and the contents of digital devices § 7.4.2.4.2.
- private search doctrine's application to digital devices § 7.6.2.2.
- government replication of a private search § 7.6.3.
- application of the search incident to arrest doctrine to cell phones and other digital devices § 8.7.
- border search doctrine's application to data and digital devices § 10.2.2.
- inventory searches § 10.8.
- requirements for computer search warrants to issue § 12.2.2.
- varieties of computer searches § 12.4.8., with subsections discussing the lower courts' fundamentally opposed views on how to treat searches for data
- time periods for warrants to be executed § 12.5.2.1.
- when probable cause becomes stale § 12.5.2.2.
- executing warrants for intermingled documents/data; off-site searches § 12.5.6.