Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

COUNTRY REPORT: UNITED STATES OF AMERICA∗

Stephen C. Thaman∗

1.THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY IN THE CRIMINAL INVESTIGATION

1.1 Introduction

Law enforcement organs in the United States (US) use information and communications technology (ICT) in conducting three types of surveillance useful for solving crimes and bringing criminals to justice: (1) the physical surveillance of people in public spaces; (2) the surveillance of transactions in which people engage; and (3) the surveillance of private communications.1

ICT is also used, however, in data mining, that is, in synthesizing and comparing data contained in large databases containing the fruits of the aforementioned three types of surveillance, in order to help sove criminal cases. Data mining can be "target-driven" and involve obtaining information about an identified suspect. It can be "match-driven" to see whether a particular person is a "person of interest." Finally, it can be "event-driven" and designed to discover the as of yet unknown perpetrator of a past event, and involves what is called "pattern-based surveillance." 2

All of these practices involve invasions of privacy of the citizenry, and thus must be discussed in light of the case law of the US Supreme Court (USSC) interpreting the extent of privacy rights in the US. After a discussion of this foundational case law, we will first look at US laws and jurisprudence in relation to the interception of the content of confidential communications, for these laws are the "gold standard" for privacy in the US. We will then discuss physical surveillance and finally transactional surveillance both to solve particular crimes and also to create massive data banks for the purpose of solving future crimes through data mining. In each of these areas, we will compare the rules for normal criminal cases, with the special regimes applying to investigations relating to national security and anti-terrorism, the data bases which are key to government criminal investigations, and the private enterprises that co-operate, voluntarily or under threat of law, with the data mining and surveillance efforts.

1.2. The Fourth Amendment Approach to Invasions of Privacy During the Criminal Investigation

The US is made up of at least 52 different jurisdictions, 50 States, one federal jurisdiction, and the District of Columbia, which has its own laws. Each State has its own codes of criminal law and procedure and constitutions, as does the federal system. Due to the muliplicity of jurisdictions, there are few general definitions of ICT, or "cyberspace"3 which apply across the board, except, perhaps, in the area of wiretapping. Otherwise, the minimal standards controlling the use of ICT in the criminal investigation in the US are derived from the case law of the USSC interpreting the Fourth Amendment (4.Amend.) of the US Constitution, which reads:

> "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."

∗ Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

∗ Saint Louis University.

1 Slobogin (2005-06, 140-41).

2 Slobogin (2008, 322-23).

3 Since 2008, The US Department of Defense (DOD) defines "cyber-space" as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." According to the Joint Chiefs of Staff of the US Armed Forces, cyber-space is: " A domain characterized by the use of electrons and the electromagnetic spectrum to store, modify, and exchange data via network [ed] systems and associated physical infrastructures." Young (2012, 20).

1.2.1 Definition of an Evidentiary "Search" for Purposes of the 4.Amend.

1.2.1.1 The "Reasonable Expectation of Privacy" Test

Prior to 1967, the definition of what was a "reasonable search" for criminal evidence under the 4.Amend, was governed by a "bricks and mortar" approach based in property law.[4] Even an "unreasonable" wiretap lacking "probable cause" was not a "search" as understood by the 4.Amend. if there was no physical intrusion onto the premises where the overheard conversations took place.[5] This changed with the decision of the USSC in 1967 in *Katz v. United States*,[6] where the court decided that the nature of the place where a private conversation takes place (in that case a phonebooth on an open street which did not conceal the person talking therein) was not dispositive, nor was the presence or not of a physical trespass, but rather whether the person surveilled had a "reasonable expectation of privacy" in the place surveilled and, in the case of wiretapping or other aural eavesdropping, in the contents of the conversations intercepted. The court enunciated that the 4.Amend. "protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of 4.Amend protection (...) But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." The definitive test from *Katz* was articulated in the concurring opinion of Justice Harlan, and it involved a two-step test: (a) that "a person exhibits an actual (subjective) expectation of privacy;" and (b) "that the expectation be one that society is prepared to recognize as 'reasonable."

Thus, if the person who is the object of the criminal investigation has no "reasonable expectation of privacy" then police investigative activities are not "searches" and are therefore not governed by the 4.Amend.

Christopher Slobogin has fashioned a handy list of factors which the USSC takes into consideration when determining whether police investigative activity constitutes a "search" within the terms of the 4.Amend. These are: (1) the nature of the place observed or inspected; (2) the steps taken by the citizen to enhance privacy; (3) the degree to which the surveillance requires a physical intrusion (trespass) onto private property, in other terms, the location of the observer; (4) the nature of the object or activity observed; and (5) the availability to the general public of any technology used by the police to conduct the surveillance.[7]

1.2.1.2 The Nature of the Place Observed: Reasonable Expectation of Privacy Applied to Activity in Public and Semi-Public Areas and Steps by Citizens to Enhance Privacy

While the 4.Amend. specifically protects "persons, houses, papers and effects" against "unreasonable searches and seizures" the protection of the "house" does not extend beyond the so-called "curtilage," that is, the "area to which extends the intimate activity associated with the sanctity of a man's home and the privacies of life." In USSC terminology, that unprotected area is called "open fields."[8] This lack of constitutional protection is justified because "there is no societal interest in the privacy of those activities, such as the cultivation of crops, that occur in fields. Moreover, as a practical matter these lands usually are accessible to the public and the police in ways that a home, and office or commercial structure would not be."[9]

But, as was noted in *Katz*, even *prima facie* protected areas, such as houses, lose their 4.Amend. protection if the owner allows access, by, for instance, leaving a marijuana plant in front of an open window which can be viewed from the street. Even the protected backyard or curtilage, which is that area closest to the house, surrounded by a fence or other enclosure,[10] is not protected if police can see into it from public areas, even if the observation point is achieved from an airplane[11] or a helicopter flying at a permissible level.[12]

A workplace is a semi-public area where a worker may have an expectation of privacy in some areas, such as a personal desk or filing cabinet, but not in other areas where employers might need access for "work-related purposes" or for the investigation of "work-related" misconduct.[13] This precedent is important for intepreting when an employee's computer files or communications might lack a protection they otherwise would enjoy. While courts have recognized that employees have a reasonable expectation of privacy in password-protected computer hard drives, some say searches of such computers may be "reasonable" under the 4.Amend. if the company which provided the computer retained access thereto and "consented" to the search by

4 Brenner (2005-06, 1).
5 Olmstead v. United States, 277 U.S. 438 (1928); Goldman v. United States, 316 U.S. 129 (1942).
6 389 U.S. 347 (1967)
7 Slobogin (1997, 390-98).
8 Hester v. United States, 267 U.S. 57 (1924).
9 Oliver v. United States, 466 U.S. 170 (1984).
10 United States v. Dunn, 480 U.S. 294 (1987).
11 California v. Ciraolo, 476 U.S. 207 (1986).
12 Florida v. Riley, 488 U.S. 445 (1989).
13 O'Connor v. Ortega, 480 U.S. 709 (1987).

government officials.14 Most courts, however, have found that employees have no expectation of privacy when using company computers for unauthorized purposes.15

1.2.1.3: The Loss of a Reasonable Expectation of Privacy Upon Relinquishing Control Over Private Information to a Third Party

1.2.1.3.1 Trash

Clearly, if one abandons an item, or a container in public, one loses any reasonable expectation of privacy. Although household or business garbage or refuse contains a wealth of information reflecting on the private personal and business life of persons, the USSC has held that a homeowner who abandons his or her garbage in opaque trashbags to the refuse collector has no expectation of privacy in the contents because "it is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."16

1.2.1.3.2 Giving Information to Current or Would-Be Government Informants: Assumption of the Risk of Loss of Confidentiality

American criminal investigators have long used undercover police or informants to penetrate into homes and other protected areas to observe activity and record conversations. Originally, a "wired" informer who was invited into a private house was not a "trespasser" and therefore the entry and use of recording devices was deemed not to violate the 4.Amend.17 Later, however, the USSC deemed that a person who invites someone into a home, or into a conversation, "assumes the risk" that that person will disclose the contents of conversations or observations, and therefore has sacrificed any "reasonable expectation of privacy."18

1.2.1.3.3 Giving Private Information to a Service Provider for Use Only in Providing the Service

The USSC has long held that a person using a bank or other financial institution has no reasonable expectation of privacy in information about his or her financial dealings, because that information is communicated to bank personnel.19 The same logic was then was applied to deny citizens a reasonable expectation of privacy in the telephone numbers they dial.20 This enables law enforcement authorities to use "pen registers" to collect numbers dialed by a suspect and "trap and trace" devices to find the numbers of those who telephone the suspect. The analogy has been made with letters mailed through the postal service. The sender has no expectation of privacy in "envelope information," i.e., the address to which the letter is mailed, but does in the content.21 We will discuss how this doctrine applies to the visiting of internet websites and to the acquisition of meta-data beyong the numbers involved in a phone conversation, that are collected by telephone service providers. Although this area is heavily regulated, because accessing this information is not protected by the 4.Amend., even violation of the rules and regulations will not lead to exclusion of the evidence in a criminal trial.

1.2.1.3.4 Unknowingly Allowing Access to a Third Person

It has long been held that the 4.Amend. only restricts the actions of state officials, and that, for instance, evidence stolen by a private party and given to the government would not violate the constitution.22 The USSC has continued to recognize, that a person's reasonable expectation of privacy in the contents of a container will also be lost if a private person accidentally gains access to the container, sees contraband, and then turns the container over to the police in a closed condition.23 This doctrine has also been extended, for instance, to contraband in a person's home seen by a hired worker who had authorized access to the place the illegal items were kept, when the worker tells the police about their existence without himself removing them from the house.24

---

14 United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).
15 United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002); United States v. King, 509 F.3d 1338 (11th Cir. 2007).
16 California v. Greenwood, 486 U.S. 35 (1988).
17 On Lee v. United States, 343 U.S. 747 (1952).
18 Lopez v. United States, 373 US 427 (l963); Lewis v. United States, 385 U.S. 206 (1966); Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971).
19 California Bankers Ass'n v. Shultz, 416 U.S. 21 (l974); United States v. Miller 425 U.S. 435 (1976):
20 United States v. New York Telephone Co., 434 U.S. 159 (l977); Smith v. Maryland, 442 U.S. 735 (1979).
21 Kerr (2010, 1019).
22 Burdeau v. McDowell, 256 U.S. 465 (1921). To my knowledge, only Texas courts would suppress evidence gathered by a private citizen in violation of the laws and constitution of the State. State v. Johnson, 939 S.W.2d 586 (Tex. Crim. App. 1996).
23 United States v. Jacobsen, 466 U.S.109 (1984).
24 United States v. Paige, 136 F.3d 1012 (5th Cir. 1998).

This constitutes a dangerous undermining of the protection of the warrant requirement for searches of houses and other private spaces, such as computers. Courts have, for instance, allowed police to search the entirety of computer storage media, after a private search detected child pornography in some of the files therein,25 even when the state agents were unaware that the private party had conducted such a search!26 Some courts refuse to allow a warrantless search of a computer, however, after a private person has conducted a search thereof.27

1.2.1.4 *Sui generis* Searches That Do Not Implicate Privacy Concerns

If the nature of the activity observed by police is *only* criminal, then one can speak of a *sui generis* search. Most searches of "bricks and mortar" houses or offices, or of containers (cars, suitcases, purses) or persons are generally exploratory and will uncover not only potential evidence of crime, but also evidence unrelated to crime.

The first articulation of the USSC in relation to a search which could theoretically only detect evidence of criminality dealt with the so-called "canine sniff," i.e., the use of trained dogs to detect contraband, such as cocaine or marijuana. The USSC held that the use of such a dog to smell a suitcase was not a "search" as one has no privacy interest in the location of contraband. The court also emphasized that such a search is much less intrusive than a normal search of a physical space.28 Since no "search" for evidence occurred, one did not need probable cause. The USSC later extended this rule to canine sniffs of automobiles.29

The only other such *sui generis* search found by the USSC was that of testing a powder substance to determine if it contained cocaine or some other prohibited drug,30 a rather banal application of the rule which is of little practical importance.

1.2.2 Development of the Search Clause and the Reasonableness Clause of the 4.Amend.

1.2.2.1 Requirement of Probable Cause and Judicial Authorization for Evidentiary Searches

The 4.Amend. clearly requires that search warrants must be based on probable cause. In the seminal case of *Illinois v. Gates*31, the USSC stated: "The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or Evidence of a crime will be found in a particular place." The requirement of "probable cause" has been extended, as well, and is required for any searches for evidence of crime or criminal suspects, and any seizures of such evidence or arrests of such suspects, whether or not judicial authorization (a warrant) is required by the law.

A search warrant must also specifically describe the place to be searched and the items to be seized. This requirement is fairly self-explanatory when applied to a specific house and specific contraband, or fruits or instrumentalities of conventional crimes. It becomes more problematic when dealing with searches of "containers" which may contain hundreds if not thousands of separate containers, such as the files in a lawyer's office, as was the case in *Andresen v. Maryland*, 32 where a search warrant arguably did not narrow the search to the particular issues under investigation. The USSC held that police searchers may look superficially through all files to determine whether any actually pertain to the alleged criminality which gave rise to the search warrant because few people keep documents of their criminal transactions in a folders specifically marked, for instance: "my criminal activity." The implications of this opinion relating to a lawyer's office are evident in relation to computers, which might contain hundreds if not thousands of separate "files" in any or none of which could be evidence of criminal activity.33

1.2.2.1.1. "Staleness" of Probable Cause and Tardiness of Execution of Search Warrants

Another issue implicating the validity of search warrants for digital or computer-stored evidence is that of "staleness." Clearly, in relation to evidence of a violent crime or drug trafficking, information that items are at a particular location on one day, does not mean they will be there 10 days later. Search warrants are therefore sometimes found to be invalid because the evidence of probable cause is too old. In relation to possession of computer files, particularly those containing illegal child pornography, courts tend to stretch the limits of the "staleness" doctrine by claiming that pedophiles or users of child pornography will seldom

25 United States v. Runyan, 275 F.3d 449 (5th Cir. 2001); Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012).
26 United States v. Oliver, 630 F.3d 397 (5th Cir. 2011).
27 United States v. Crist, 627 F.Supp. 2d 575 (M.D. Pa. 2008)
28 United States v. Place, 462 U.S. 696 (1983).
29 Illinois v. Caballes, 543 U.S. 405 (2005).
30 United States v. Jacobsen, 466 U.S. 109 (1984)
31 462 U.S. 213 (1983).
32 427 U.S. 463 (1976).
33 Clancy (2005-06, 195-98).

delete such files once they possess them. Thus courts have upheld searches of homes and computers located in homes many months after images were allegedly e-mailed to the computer or downloaded.34

Statutes also usually require a search to be conducted within 10 days of the issuance of a search warrant.35 Thus, when a search warrant authorizes the "seizure" of a computer from a home and the "search" of its contents, the question arises as to whether the search must also be within, say, 10 days of the seizure of the computer.36 Some courts, however, when issuing a warrant, will specifically give law enforcement additional time to conduct the search of the computer drives.37 In some cases, police must also seek a separate search warrant to search the contents of a computer, which it might have lawfully seized pursuant to a broad search for "records" or indicent to arrest without a warrant.38

1.2.2.1.2 Old Restriction of Seizure of "Mere Evidence"

Prior to 1967, the USSC recognized a prohibition on the seizure of any evidence that was not contraband, instrumentalities of crime or fruits of crime (such as stolen goods). Thus, personal papers, diaries, even business records were subject to a *Beweiserhebungsverbot*. In a famous nineteenth century case, the USSC ruled that not only could private papers not be seized, but that search warrants could not be issued to even look for them in a private dwelling. Looking at a man's papers was also considered to violate the privilege against self-incrimination guaranteed by the Fifth Amendment of the US Constitution (5.Amend.) and the USSC felt that allowing the reading of private documents would hurt the innocent even more than the guilty.39 This changed with the decision of *Warden v. Hayden*,40 which held that any evidence, even circumstantial evidence of guilt, could now be seized if the 4.Amend. was not otherwise violated, for, since *Katz*, the emphasis had now shifted to protection of privacy and not property. This sea change obviously has opened the door to the seizure of digital evidence, as long as there is no violation of the 4.Amend.

1.2.2.1.3 The "Plain View" Doctrine: Accidental Discoveries During a Legal Search

If police are validly on a premises for purpose of making a search, or validly searching a computer for specific material, whether as a result of a search warrant or another accepted "reasonable" search under the 4.Amend., they may also seize evidence the search warrant or previous probable cause did not authorize them to seize, if, upon seeing it, it is clearly contraband, fruits, instrumentalities, or other obvious circumstantial evidence of crime.41 If the searching officer has to do any further "search," no matter how minimal,42 to determine whether the object is related to crime, then the seizure of the item is invalid and it may not be used in court. This doctrine is now crucial in determining whether officers searching for digital evidence, may open other files in the same computer hard drive.

1.2.2.1.4 Exception for "Exigent Circumstances"

As in all countries, if police have probable cause to enter or search a place, but do not have time to get a search warrant due to emergency or exigent circumstances, then the search is still legal. This applies to entering a dwelling to arrest or "seize" a fleeing person,43 to arrest a person suspected of a dangerous crime if there is danger in delay of escape or violence,44 or to search for evidence that might be easily destroyed.

---

34 5 months in State v. Felix, 942 So.2d 5 (Fla. App. 2006); 5 ½ months in United States v. Lamb, 945 F.Supp. 441 (N.D.N.Y. 1996); 18 months in United States v. Lemon, 590 F.3d 612 (8th Cir. 2010). One court has said that a warrant should be denied in child porn cases only in "exceptional cases." United States v. Seiver, 692 F.3d 774 (7th Cir. 2012).

35 Fed. R. Crim. P. 41(c); Vernon's Annotated Missouri Codes: § 542.276.8. 10 days is also the limit in California, whereas in Illinois, a search warrant must be served within 96 hours of issuance. 725 ILCS 5/108-6.

36 Whereas in the State of Washington, the computer search may take place after the 10 days have elapsed. State v. Grenning, 174 P.3d 706 (Wash. App. 2008), one federal court suppressed evidence where police held computers over a year before searching them . United States v. Metter, 860 F.Supp.2d 205 (E.D.N.Y. 2012).

37 United States v. Sypers, 426 F.3d 461 (1st Cir. 2005)(allowing a 5 month delay). Another 5 month delay was allowed in United States v. Christie, 717 F.3d 1156 (10th Cir. 2013). On the length of time required for computer experts to search a computer hard-drive and the problems of keeping within the 10 day-rule, see Kerr (2005-06, 92-95-102-04).

38 In one case, a search warrant was denied because the police waited 21 days after seizing the computer to apply for the warrant. United States v. Mitchell, 565 F.3d 1347 (11th Cir. 2009).

39 Boyd v. United States, 116 U.S. 616 (1886).

40 387 U.S. 294, 301-302 (1967).

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

42 I.e., such as turning over a phonograph turntable to find a serial number, Arizona v. Hicks, 430 U.S. 321 (1987).

43 Warden v. Hayden, 387 U.S. 294, 301-302 (1967).

44 Minnesota v. Olson, 495 US 9l (l990)(holding, however, that this does not apply to every murder case).

The USSC has also recognized a general exception for automobiles, which was originally based on their "moveability,"45 but now applies even if the automobile has been towed and otherwise immobilized by the police.46 This exception for "moveability" has never, however, been applied to smaller portable items, such as purses, suitcases or computers.47

1.2.2.1.5 Consent Search: Exception to Probable Cause and Warrant Requirements

While consent searches are exceptions to the requirement of judicial authorization in all countries, they are facilitated in the US by the fact that the USSC does not require that police advise the person whose house, car, possessions or person they want to search, that the person has the right to refuse to consent.48 If a person has been seized in violation of the 4.Amend., however, a subsequent consent to search will usually be deemed to be "fruit of the poisonous tree" and the evidence seized will be inadmissible. Consent of one person who participates in a confidential conversation will also eliminate the requirement of a judicial order to intercept such conversation.

A person may also consent to the search of premises which he or she owns or controls along with third persons, inasmuch as the latter have "assumed the risk" of that person giving others access to the jointly owned property. In the case of dwelling searches, however, the police may not rely on the authorization of one person to search jointly-owned or occupied premises if another co-owner or co-occupier is present and objects to the search.49 Police may also rely on consent given by a person who appears to have control of property, as long as the police reasonably believe she does have such control.50 Third-party consent is important in relation to searches of computers which are used by more than one party.

1.2.2.2 "Reasonable" Seizures and Searches under the 4.Amend. Which Do Not Require Probable Cause or Judicial Authorization

1.2.2.2.1 Temporary Detentions Based on Reasonable Suspicion

One of the first interpretations of the "reasonableness clause" of the 4.Amend. was in *Terry v. Ohio*,51 in which the USSC, applying a proportionality test, declared that a short-term detention of a person for the purpose of investigating past or on-going crime could be based on less suspicion than the "probable cause" articulated in the 4.Amend, because such a detention was a lesser intrusion than a full-scale arrest. The standard for this lesser suspicion was called "reasonable suspicion." If, however, police detain a suspect without reasonable suspicion, i.e., just based on a hunch or stereotype, then any statements made by that person or evidence found as a result of a search can not be used in court, because the temporary detention violated the 4.Amend.

1.2.2.2.2 Protective Searches Based on Reasonable Suspicion

In *Terry*, the USSC also held that police may, after they have lawfully detained a person for investigation upon reasonable suspicion, carefully pat-search the person's outer clothing for weapons if they can articulate a second "reasonable suspicion" that the person is armed and dangerous. Again, the lesser-intrusion of a superficial pat-search of clothing could be justified on a lesser standard of suspicion than "probable cause."

With *Terry*, the USSC began to use the "probable cause" standard for searches for evidence, and the "reasonable suspicion" standard for protective searches. The reasonable suspicion standard was also later applied to searches of vehicles for weapons,52 search of houses for dangerous accomplices following an arrest of a suspect in such a house,53 or searches of dwellings for the purpose of protecting life or property, rather than explicitly for criminal evidence.54

1.2.2.2.3 Searches Incident to Arrest

In America, a person arrested has traditionally been searched immediately following the arrest. However, the law was unclear as to the extent of such a search, especially when an arrest took place in a dwelling, until the USSC decided in 1969 that the police could search not only the person of an arrestee, but also "the area into which an arrestee might reach in order to grab a weapon

45 Caroll v. United States, 267 U.S. 132 (1925).
46 Chambers v. Maroney, 399 U.S. 42 (1970).
47 United States v. Chadwick, 433 U.S. 1 (1977).
48 Schneckloth v. Bustamante, 412 U.S. 218 (1973)
49 Georgia v. Randolph, 547 U.S. 103 (2006).
50 Illinois v. Rodriguez, 497 U.S. 177 (1990).
51 392 U.S. 1 (1968).
52 Michigan v. Long, 463 U.S. 1032 (1983).
53 Maryland v. Buie, 494 U.S. 325 (1990)
54 Brigham City, Utah v. Stuart, 547 U.S. 398 (2006).

or evidentiary item."55 The rationale was the "exigent circumstance" of preventing an arrestee from reaching either a weapon to use against the arresting officer, or evidence which could be destroyed.

The USSC later dropped the "exigent circumstance" underpinning of the rule and allowed officers to automatically search the person of all arrestees56 and, if they were arrested either in or shortly after having exited an automobile, the entire passenger compartment of the automobile, including containers therein, whether or not the officer was in fear of a weapon or of evidence being destroyed. 57

USSC opinions which permitted custodial arrests following violations of minor traffic offenses,58 and the stopping of cars involved in minor traffic violations as a pretext to investigate narcotics offenses,59 enabled police to very easily convert a minor traffic stop into a full evidentiary search of the driver and all containers in the passenger compartment of a car without any reasonable suspicion or probable cause. This doctrine was used, as well, to search electronic apparatuses, such as computers, cellphones,60 and pagers,61 although some courts felt the very personal nature of the contents of such "containers" protected them from the reach of the exception for searches incident to arrest.62

In 2009, however, the USSC placed stricter limitations on searches of automobiles incident to arrest, holding that if the arrest took place while the person was in the car, the police could search the passenger compartment of the car for weapons, but that if the arrest was made outside the car, the police could only search the passenger compartment if their were reasonable suspicion that evidence *of the crime for which the person was arrested* could be found therein.63

This stricter rule would, in my opinion, make searches of computers, cellphones or pagers illegal if the arrest were for something like a violation of the rules of the road or was based on an old arrest or bench warrant.64 Yet, following *Gant* some courts are still allowing searches of electronic "containers" even under the more restrictive current test.65 The content of most containers is restricted, however, to their physical space. In this sense, computers, I-phones, etc., are different, as one can use them to access information not contained within the physical confines of the electronic hardware. It appears, however, that no court has yet allowed police to use a computer or I-phone seized incident to arrest, to access contents that are not contained in the hard drive of the computer itself.66

1.2.2.2.5 Individual Searches Based on Less than Probable Cause

The USSC has allowed such searches but has two theories justifying them. The first is that administrative "special needs" not related to criminal law enforcement justify certain searches based on less than probable cause.67 The second theory is uses simple proportionality analysis, as was used in *Terry v. Ohio*, to determine whether a search is "reasonable," i.e., if there is a lesser expectation of privacy or a less intrusive search, it may be based on less than probable cause.

1.2.2.2.5.1 Administrative "Special Needs" Analysis

The USSC has allowed public school officials to authorize the search of minor students on school campuses, if they have an "individualized" reasonable suspicion that the student is committing a crime or otherwise violating school rules. This lower standard for a search which could produce criminal evidence was justified by the "special need" to maintain order and an environment conducive to learning in the schools.68 The USSC also found that a "special need" justified the warrantless searches of the houses and effects of persons on probation based only on "reasonable suspicion" to facilitate probation

55 California v. Chimel, 395 U.S. 752 (1969)
56 United States v. Robinson, 414 U.S. 218 (1973).
57 New York v. Belton, 453 U.S. 454 (1981); Thornton v. United States, 541 U.S. 615 (2004).
58 Atwater v. City of Lago Vista, 532 U.S. 318 (2001).
59 Wrenn v. United States, 517 U.S. 806 (1996).
60 United States v. Finley, 477 F.3d 250 (5th Cir. 2007).
61 United States v. Chan, 830 F.Supp. 531 (N.D.Cal. 1993); United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996).
62 State v. Smith, 920 N.E.2d 949 (Ohio 2009).
63 Arizona v. Gant, 556 U.S. 332 (2009)
64 For a case rejecting the "automatic" search of the contents of arrestee's cellphones: Smallwood v. State, 113 So.3d 724 (Fla. 2013); see also United States v. Wurie, 1st Cir., No. 11-1792, 5/17/13)(not yet reported).
65 People v. Diaz, 244 P.3d 501 (Cal. 2011). Applied to cellphones: People v. Nottoli, 130 Cal. Rptr. 3d 884 (Cal. App. 2011); United States v. Curtis, 635 F.3d 704 (5th Cir. 2011); United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012); Hawkins v. State, 723 S.E.2d 924 (Ga. 2012)(arrest for drugs after officer used text-messages to arrange drug sting);
66 Brenner (2012A, 533-34).
67 New York v. Burger, 482 U.S. 691 (1985)(involving administrative searches of auto junkyards).
68 New Jersey v. T.L.O., 469 U.S. 325 (1985).

supervision and based the lesser standard on the lesser expectation of privacy a probationer enjoys due to his or her status.69 Such a "special needs" rationale has been used to justify, as a condition of probation in a child pornography case, the installation of a device that would monitor or filter the probationer's computer use.70

In a 2006 case, the USSC held that persons on parole after having served part of a prison sentence could be searched without any suspicion at all because of their greater propensity to commit future offenses. The Court did not justify this search on the "special need" to supervise parolees, but simply found it to be "reasonable" under the 4.Amend.71 This is one area where some courts rely on the "special need" to ensure an effective operation of the parole system72 and others just base the decision on proportional "reasonableness."

One court also deemed that protection of a government e-mail server qualified as a "special need" justifying a warrantless remote accessing of a personal computer in the dormitory room of a state university student suspected of being a hacker.73

1.1.2.2.5.2 Individual Searches Based on Reasonableness Clause Balancing (Proportionality)

In a recent case, the USSC held that a search conducted by a government employer (in this case a police department) of an employee's pager is simply "reasonable" under the 4.Amend if done "for non-investigatory, work-related purposes as well as for investigations of work-related misconduct." Such a search of work-related spaces or electronic tools, such as pagers or computers is "reasonable" if "the measures adopted are reasonable related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search."74

Although some states, including New York, Delaware and Connecticut, have recently passed statutes requiring employers to notify employees when monitoring their electronic communications, the USSC in *Quon* did not say this was required.

Another long-recognized "reasonable" search which does not require any particularized suspicion or a warrant is a customs search of mail, packages, or persons and their belongings when entering or leaving the US.75 There was a time when it was thought that a letter could be opened, to discover whether it contained contraband, upon entering the country, but not that it could be read. Today, however, some courts allow customs officials to actually read the contents of letters which enter the US.76

Some courts also deem that a search of a laptop, its harddrive and computer disks, is justified without particularized suspicion under the exception for customs searches, if a person is carrying them when entering the country.77 Other courts, however, require that there at least be an individualized reasonable suspicion for a such of laptop computers, smartphones or other digital media brought across the border by travelers.78

From Oct. 1, 2008 through June 2, 2010, 6,671 travelers, 2,995 of them American citizens, had electronic gear searched upon entering or leaving the US. Sometimes the electronic hardware was kept for weeks to do a thorough analysis of its contents.79

1.2.3 The Inadmissibility of Evidence Seized in Violation of the 4.Amend.

1.2.3.1 History of the 4.Amend. Exclusionary Rule and Its Extention to the "Fruits of the Poisonous Tree"

Traditionally in Common Law countries, courts did not inquire into the means by which otherwise relevant and material evidence was acquired.80 But in 1914, the USSC noted the expansive violations of constitutional rights by federal officials both in conducting searches and seizures and during police interrogations, and decided that, without a rule mandating exclusion of evidence seized in violation of the 4.Amend. " the protection of the 4.Amend. right to be secure against such searches and seizures is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution."81

69 United States v. Knights, 534 U.S. 112 (2001).
70 United States v. Lifshitz, 69 F.3d 173 (2d Cir. 2004); United States v. Yuknavich, 419 F.3d 1302 (11th Cir. 2005).
71 547 U.S. 843 (2006).
72 People v. McCullough, 6 P.3d 774 (Colo. 2000).
73 United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007).
74 City of Ontario v. Quon, 130 S.Ct. 2619 (2010)
75 United States v. Ramsey, 431 U.S. 606 (1977).
76 United States v. Seljan, 547 F.3d 993 (9th Cir. 2008).
77 United States v. Ickes, 393 F.3d 501 (4th Cir. 2005); United States v. Arnold, 533 F.3d 1003 (9th Cir. 2008).
78 United States v. Cotterman, 709 F.3d 952 (9th Cir. en banc 2013).
79 Shipler (NYT, 20 Feb 2011).
80 Adams v. New York, 192 U.S. 585 (1904).
81 Weeks v. United States, 232 U.S. 383 (1914).

Some States followed the USSC and also excluded evidence gathered in violation of their own constitutional protections against unreasonable searches and seizures and others did not, but in 1961, the USSC made the *Weeks* exclusionary rule binding on the States in *Mapp v. Ohio*, after determining that other remedies, such as suits in tort, or police discipline were ineffective means of deterring police violations.82 The *Mapp* court based the exclusionary rule on the need for deterring police illegality, but also on "the imperative of judicial integrity," emphasizing that "nothing can destroy a government more quickly than its failure to observe its own laws, or worse, its disregard of the charter of its own existence."

Even before *Mapp* the USSC coined the term "fruits of the poisonous tree" to indicate that evidence which was seized as the indirect result of a 4.Amend. violation would also have to be excluded from the trial unless the connection between violation and "fruit" may "have become so attenuated as to dissipate the taint."83 Again in 1954, the USSC emphasized that, in regard to evidence seized in violation of the 4.Amend, the government cannot "make indirect use of such evidence for its case, or support a conviction on evidence obtained through leads from the unlawfully obtained evidence. All these methods are outlawed, and convictions obtained by means of them are invalidated, because they encourage the kind of society that is obnoxious to free men."84

Some common potential applications of the doctrine of the fruits of the poisonous tree to ICT information would be: (1) when an illegal search, arrest, or interrogation leads to evidence that constituted the probable cause for either a warrant to seize and search a computer, or a warrant under Title III to intercept confidential communications; (2) when an illegal arrest or detention leads to the seizure and search of a computer, cellphone, or I-phone; (3) when an unlawful interception of communications leads to the discovery of witnesses or physical evidence that is used against the subject of the interception or a third party.

1.2.3.2 Modern Exceptions to the 4.Amend. Exclusionary Rule

1.2.3.2.1 The "Independent Source" Exception

Evidence is deemed not to be the "fruit" of a 4.Amend. violation if a second, sufficiently independent legal investigative action actually led to the seizure of the evidence after an unlawful investigative act had discovered its existence.85 This does not mean, however, that officers may make an illegal "preview search" of a suspect's computer in order to obtain information for a search warrant which then later seizes the files in the computer.86

Some jurisdictions have limited the exception for "independent source" to cases where there is no connection between the initial illegality and the subsequent legal measure, i.e., when it is not the same police unit that is involved in both illegal and legal measures.87

1.2.3.2.2 The "Inevitable Discovery" Exception

If there is only one search or seizure, and it violates the 4.Amend., or even if there is an illegal interrogation which leads to the discovery of physical evidence, the physical evidence will not be inadmissible if the court determines that the physical evidence would inevitably have been discovered by legal means regardless of the violation which actually led to its discovery.88

1.2.3.2.3 The Good Faith Exception

The USSC has also denied exclusion of illegally gathered evidence when the the police officer acted in "good faith" in conducting the investigative measure which discovered the evidence because excluding the evidence would thus not serve to deter future police misbehavior. In *United States v. Leon*,89 the USSC first applied this doctrine to a case where the judge blundered by issuing a search warrant based on insufficient probable cause. In *Leon*, the USSC abandoned the "judicial integrity" reason for the exclusionary rule in favor of focusing solely on police deterrence. The USSC has also applied this exception to errors made in describing the things to be seized, or the premises to be searched, as well as other technical errors in warrants. 90

82 Mapp v. Ohio, 367 U.S. 643 (1961).
83 United States v. Nardone, 308 U.S.338(1938).
84 Walder v. United States, 347 U.S. 62 (1954).
85 Murray v. United States, 487 U.S. 533 (1988)(illegal entry of warehouse due to lack of exigent circumstances led to discovery of marijuana but search warrant based on independent evidence of the presence of the marijuana subsequently led to its seizure).
86 State v. Nadeau, 1 A.3d 445 (Me. 2010).
87 Commonwealth v. Melendez, 676 A.2d 226 (Pa. 1996); State v. Wagoner, 24 P.3d 306 (N.M.App. 2001).
88 Nix v. Williams, 467 U.S. 431 (1984)
89 468 U.S. 897 (1984)
90 Massachusetts v. Sheppard, 468 U.S. 981 (1984).

In applying these exceptions, for instance, a computer search based on an overbroad warrant in violation of the 4.Amend., might not lead to suppression of the incriminating files discovered due to the "good faith" exception.91

"Good faith" led in *Arizona v. Evans*, to admission of evidence seized as the result of an error in ICT information conveyed by a court computer system that indicated that a warrant existed to arrest a suspect.92 Justice Ginzburg in *Evans* dissented, claiming that the widespread use of computers by courts and police departments and the unreliability of much information contained in them could lead to a huge amount of unlawful arrests.

Originally courts would not apply "good faith" it was the errors in police or other executive branch computer systems that led to an unlawful arrest,93 but only when the error was attributable to a court computer system. However, in a 2009 case the USSC found "good faith" even when the arresting officers' negligence played a role in the mistaken arrest.94

1.2.3.2.4 "Standing" Limitations on Ability to Move to Suppress Evidence

In 4.Amend. case law, following the *Katz* decision, one has "standing" to litigate a search only when one has a "reasonable expectation of privacy" in the place searched, whereas prior to that decision it was sufficient to assert a property interest in the item seized.95 As the California Supreme Court once stated, this doctrine "virtually invites a law enforcement officer to violate the rights of third parties and to trade the escape of a criminal whose rights are violated for the conviction of others by the use of the evidence illegally obtained against them."96

In the context of wiretapping, the USSC held in 1969 that only those whose rights were violated by a wiretap had the standing to move to suppress illegally gathered information, but not those who were solely damaged by the introduction of the evidence in court. Standing would be accorded to anyone who participated in the conversation or whose telephone was actually tapped.97

In relation to searches of homes (including installation of bugs or secret cameras), the USSC accords standing to the legal residents of the home as well as any overnight visitors,98 but not necessarily to short term visitors in a home or other private spaces, especially when they are conducting illegal business.99 Some courts have, however, accorded short-term business visitors to a hotel room a reasonable expectation that they will not be videotaped in the host's absence.100

In relation to automobiles, although the *Rakas* majority would only have accorded standing to the owner of a vehicle, and not to invited passengers, other courts extend a right of privacy to non-owner drivers and sometimes to passengers as well. The standing issues relating to automobiles are important in an era where GPS monitoring of automobiles, and even the use of built-in monitoring devices to record conversations in automobiles are tools of law enforcement.

Fraudulent acquisition or possession of an automobile or computer, however, has been held to deprive the possessor of any expectation of privacy in the vehicle, or in the contents of the computer.101 One court, however, has held that obtaining telephone service through use of a false name did not deprive the person of an expectation of privacy or protection of the State's wiretap laws.102

1.2.3.2.5 Use of Illegally Seized Evidence to Impeach a Testifying Defendant

The USSC has allowed evidence seized in violation of the 4.Amend. to be used to impeach the testimony of the defendant,103 but, oddly enough, has not allowed such use to impeach the testimony of a witness.104

1.2.3.2.6 Limitations on the 4.Amend. Exclusionary Rule to the First Instance Trial

Generally speaking, evidence gathered in violation of the 4.Amend. is inadmissible at trial in the first instance, but is admissible in a number of other judicial and non-judicial proceedings. Thus, at proceedings before a grand jury, the purpose of which is to

91 See United States v. Otero, 563 F.3d 1127 (10th Cir. 2009).
92 514 U.S. 1 (1995)
93 State v. White, 660 So.2d 664 (Fla. 1995); State v. Hisey, 723 N.W.2d 99 (Neb. App. 2006).
94 Herring v. United States, 555 U.S. 135 (2009).
95 Rakas v. Illinois, 439 U.S. 128 (1978)
96 People v. Martin, 290 P.2d 855, 857 (Cal. 1955)(no longer good law).
97 Alderman v. United States, 394 U.S. 165 (1969)
98 Minnesota v. Olson, 495 U.S. 91 (1990)
99 Minnesota v. Carter, 525 U.S. 83 (1998)
100 United States v. Nerber, 222 F.3d 597 (9th Cir. 2000).
101 United States v. Caymen, 404 F.3d 1196 (9th Cir. 2005).
102 People v. Leon, 32 Cal. Rptr. 3d 421 (Cal. App. 2005).
103 United States v. Havens, 446 U.S. 620 (1980).
104 James v. Illinois, 493 U.S. 307 (1990).

assess the sufficiency of evidence to charge a suspect, illegally seized evidence may be used.105 The exclusionary rule also does not apply in some cases to sentencing proceedings,106 or to proceedings on *habeas corpus* to challenge final convictions.107 It also does not apply to hearings to violate a person's probation or parole,108 or to non-criminal deportation109 or military discharge110 proceedings.

1.2.3.3 Exclusionary Rule Conflicts Between States and Between State and Federal Courts

1.2.3.3.1 Approach of Federal Courts Where State Law is More Protective than the Fourth Amendment

Many States have stricter protections against government search and seizure than the minimum requirements imposed by the USSC. However, nearly all federal courts will still accept evidence gathered in accordance with the minimal 4.Amend. norms, even though State officials violated their State's stricter rules, and turned the evidence over to the federal officials.111

1.2.3.3.2 Where State Law Gives No More Protection than Federal Law

In the 1980s, the people of California, through a referendum, decided that the California constitution could give no greater protection than the minimal protection determined by the USSC in its interpretation of the 4. Amend. Thus, even when California police violate a California law which gives more protection than the 4.Amend. as interpreted by the USSC, the California courts will not exclude the evidence illegally gathered.112

1.2.3.3.3 Approach of States Which Give More Protection than Federal Law or the Law of Other States

Some States which accord more protection than the federal government, or other States, will still allow its courts to use evidence gathered by officials of the less-protective jurisdictions, even if the gathering of the evidence would have violated its State constitution, because the chief purpose of their stricter exclusionary rules is to deter their own State officials from violating State law.113 If officers of a state granting more protection participate in a search in a jurisdiction according less protection, then these States will apply their own exclusionary rule.114 Other States will exclude the fruits of searches conducted in a jurisdiction the standards of which give less protection than their constitutions, regardless of whether the search was carried on by the less-protective jurisdicition's officers.115

1.3 The Interception of Private Communications and Metadata

1.3.1 Wiretapping and Bugging

1.3.1.1 History

Early federal and state law prohibited wiretapping or any interception and divulgation or publishing of contents of any communications by telegraph or telephone.116 Even though federal and state officials engaged in massive illegal wiretapping unbenknownst to the citizenry,117 the USSC early held that the tapping of telephone convesations did not constitute a violation of the 4.Amend. as long as federal officials did not actually trespass on the suspect's property.118 Justice Brandeis, in one of

105 United States v. Calandra, 414 U.S. 338 (1974).
106 United States v. Tejada, 956 F.2d 1256 (2d Cir. 1992); United States v. Brimah, 214 F.3d 854 (7th Cir. 2000). The exception is when officers obtained the evidence specifically to enhance an upcoming sentence. Verdugo v. United States, 402 F.2d 599 (9th Cir. 1968).
107 Stone v. Powell, 428 U.S. 465 (1976).
108 Pennsylvania Board of Probation and Parole v. Scott, 524 U.S. 357 (1998). Some States, however, do not allow use of illegally gathered evidence at parole or probation hearings. State v. Marquart, 945 P.2d 1027 (N.M. App. 1997); State v. Scarlet, 800 So.2d 220 (Fla.2001).
109 INS v. Lopez-Mendoza, 468 U.S. 1032 (1984)
110 Garrett v. Lehman, 751 F.2d 997 (9th Cir. 1985).
111 United States v. Bell, 54 F.3d 502 (8th Cir. 1995); United States v. Appelquist, 145 F.3d 975 (8th Cir. 1998); United States v. Vite-Espinoza, 342 F.3d 462 (6th Cir. 2002); United States v. Laville, 480 F.3d 187 (3d Cir. 2007); United States v. Graham, 553 F.3d 6 (1st Cir. 2009); United States v. Beals, 698 F.3d 248 (6th Cir. 2012).
112 People v. McKay, 41 P.3d 59 (Cal. 2002).
113 State v. Bridges, 925 P.2d 357 (Haw. 1996); State v. Torres, 252 P.3d 1229 (Haw. 2011).
114 State v. Mollica, 524 A.2d 1303, 1305-06 (N.J.App 1987); State v. Torres, 252 P.3d 1229 (Haw. 2011).
115 For a discussion, see Brenner (2012, 56-59).
116 § 605 Federal Communications Act of 1934; Nardone v. United States, 302 U.S. 379 (1937)(case famous for the coining of the term "fruits of the poisonous tree."
117 This was documented in a famous investigation published in 1959. Samuel Dash, Richard F. Schwartz & Robert E. Knowlton, The Eavesdroppers (1959), cited in Freiwald (2004, 11-12).
118 Olmstead v. United States, 277 U.S. 438 (1928).

the most famous dissents in USSC history, claimed that the content of a telephone conversation should have the same protection already given by the USSC to the contents of letters.119

Brandeis noted that: "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping." In his dissent, he made the most eloquent defense of citizen privacy against illegal government meddling therein:

> "(The) makers of our Constitution..conferred, as against the government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the govt upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth Amendment."
>
> "Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the governmentt will be imperiled if it fails to observe the law scrupulously. Our governmentt is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means--to declare that the government may commit crimes in order to secure the conviction of a private criminal--would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face."

Illegal wiretapping was was often conducted with the cooperation of local phone companies, who conspired with agents to keep surveillance secret in order to maintain public confidence in the telephone networks. This rampant and widespread illegal use of wiretapping by both federal and state law enforcement agents reflects the historical ambivalence towards electronic surveillance in the U.S.120

With the decision in *Katz*121 in 1967, which held that the wiretapping of the suspect in a telephone booth would have been legal, had the police acquired judicial authorization, and another case in the same year which invalidated New York State's wiretap statute due to the vagueness of the prerequisites it imposed,122 the stage was set for legislation regulating the government's use of wiretapping and bugging, which would come the next year in 1968.

1.3.1.2 Title III: the Federal Wiretap Law

In 1968 Congress enacted the Omnibus Crime Control and Safe Streets Act, Title III of which contained the new wiretap legislation, which thereafter was simply known as "Title III."123 Title III pre-empted the field, setting guidelines not only for the federal government, but also for the States. State wiretap law may not impose less control over the use of wiretaps and bugs than does federal law.

In 1986 Congress amended Title III with the Electronic Communications Privacy Act (ECPA) to modernize the law and make it applicable to the advent of cell phones and internet communication. Title I of ECPA included the provisions for interceptions of wire and electronic communications, Title II of ECPA dealt with stored communications and is known as the Stored Communications Act (SCA), and Title III of ECPA deals with accessing communications metadata and is known as the "Pen Register Act."124

Title III (I will continue using that term) imposes a felony sanction of up to five years imprisonment or a fine, or civil sanctions for the illegal interception or divulgation of any wire, oral or electronic communications through wiretaps, installation of bugs (listening devices) or any other means,125 as well as for possessing, transporting or even advertising devices which can be used for illegal interceptions of such conversations.126

"Electronic communication, " within the meaning of Title III, includes "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

119 Ex parte Jackson, 96 U.S.727 (1877).
120 Freiwald (2004, 11-12, 26-27).
121 Katz v. United States, 389 U.S. 347 (1967).
122 Berger v. New York, 388 U.S. 41 (1967).
123 Pub. L. 90-351, 82 Stat. 197.
124 Solove (2002, 1139-40).
125 18 U.S.C. §§ 2511(1)(a); 2511(4)(a).
126 18 U.S.C. § 2512

system," but does not include: wire or oral communication, communications made through a tone-only paging device,127 or from a tracking device.128 Title III explicitly does not apply to the use of pen registers or trap and trace devices which record external telecommunications data, such as numbers dialed.129

"Interception" within the meaning of Title III includes eavesdropping contemporaneous with the transmission of communications,130 but not the accessing of stored private e-mail sent to a service provider, which had not yet been retrieved,131 nor the recording of an instant message (IM), because an IM service creates a paper trail of a dialog, and thus using that form of communication amounts to giving implied consent for the other party to record the stream of the conversation. 132

There has been some dispute as to whether electronic communications in the form of e-mail or text messages can actually be "intercepted" under Title III. As one court asserted, there 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" and thus held interception to be virtually impossible "unless some type of automatic routing software is used."133 One court, however, did rule that the unauthorized interception of an electronic mail message in temporary, transient storage violated Title III,134 though the prevailing view is that its seizure is governed by the SCA.

A State court has also ruled that software that surreptitiously captures images on computer screens, records chat conversations, instant messages, e-mails sent and received and websites visited, unlawfully "intercepted" electronic communications in transmission in violation of its wiretap act, holding that these electronic communications fell within the "umbra" of the wiretap law because the communications were not retrieved from storage, and thus they were "intercepted communications."135

1.3.1.2.1 Catalogue of Offenses

Wiretaps in the State courts are permissible in relation to the "commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses."136

Because of the specialized, sprawling and duplicative nature of federal criminal law, the list of offenses for which wiretapping may be employed covers several pages of the code. Included, other than those in the State list above, are offenses relating to atomic energy, nuclear facilities, biological weapons, espionage, sabotage, trade secrets, treason, riots, destruction of property and maritime vessels, piracy, corruption dealing with labor unions, bribery of public officials and bank officials, and involving sports events, violence at international airports, domestic terrorism, unlawful use of explosives, tax evasion, gambling, terrorist threats, varous types of fraud, obstruction of justice, human trafficking, organized crime and racketeering,

money laundering, sexual exploitation of children and child pornography, torture, counterfeiting or production of false documents and identifications, narcotics offenses, extortionate credit transactions and bank reporting violations, firearms violations, anti-trust violations, and any conspiracy to commit any of the above crimes.137

---

127 Otherwise a Title III order is needed to access a pager. Adams v. Battle Creek, Mich., 250 F.3d 980 (6th Cir. 2001); Brown v. Waddell, 50 F.3d 285 (4th Cir.1995). Cellular phone conversations have been protected by Title III since amendments to the law in 1994. Prior to that, police in some jurisdictions used scanners to intercept cell phone calls and did not need a warrant.
128 18 U.S.C. § 2510(12).
129 18 U.S.C. § 2511(2)(h).
130 United States v. Turk, 526 F.2d 654 (5th Cir. 1976). Though not if carried out in the back of a police car containing arrested suspects, due to the lack of a reasonable expectation of privacy. United States v. Turner, 209 F.3d 1198 (10th Cir. 2000); United States v. Clark, 22 F.3d 799 (8th Cir. 1994); State v. Timley, 975 P.2d 264 (Kan. App. 1998); State v. Torgrimson, 637 N.W.2d 345 (Minn.App. 2002). Even if the arrested suspects asked to speak privately. State v. Scheineman, 77 S.W.3d 810 (Tex. Crim.App. 2002). Prisoners also have no right to privacy in their telephone calls, and therefore no "interception" is recognized. United States v. Hammond, 286 F.3d 189 (4th Cir. 2002). Lawyers, however, who receive calls from imprisoned clients have a reasonable expectation of privacy in these phone calls and a civil cause of action against prison officials who overhear them. United States v. Novak, 453 F.Supp.2d 249 (D. Mass. 2006); Lonegan v. Hasty, 436 F.Supp. 2d 49 (E.D.N.Y. 2006).
131 Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).
132 State v. Lott, 879 A.2d 1167 (N.H. 2005).
133 United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003).
134 United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
135 O'Brien v. O'Brien, 899 So.2d 1133 (Fla. App. 2005)
136 18 U.S.C. § 2516(2).
137 18 U.S.C. § 2516(1).

While simple prostitution is not a catalogue offense, one court has held that wiretaps may be used to investigation prostitution if it is connected with organized crime.138

Although the original version of Title III permitted wiretapping only for serious crimes that were typical of organized crime activities, Congress made no such restrictions when it came to intercepting electronic communications when it passed the ECPA in 1986. Interceptions of content may proceed in relation to the investigation of any federal felony. There are no restrictions whatsoever, when it comes to accessing stored communications or installing pen registers or trap and trace devices, other than that there be a "criminal investigation" even if it is for a misdemeanor.139

1.3.1.2.2 Requirement of Probable Cause and Judicial Control

Title III imposes stricter judicial control on interceptions of private communications than does the 4.Amend. on search warrants,140 and some call the Title III order, for this reason, a "super warrant." Only high-level prosecutors or US Attorneys (in the federal system) may apply for a judicial wiretap order under Title III, whereas any police officer may apply for a search warrant. In addition, only high court felony trial judges may issue such an order, whereas even lower courts and magistrates or even justices of the peace can issue a normal search warrant.141

Although the definition of "probable cause" for obtaining an interception of communications is considered to be identical with that for obtaining a search warrant,142 the application presented by prosecutors for an interception order is in other ways stricter than that required for a normal search warrant. It must include, besides a "full and complete statement" which amounts to probable cause, and a description of the communications facilities or locations to be intercepted, "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," and a statement of the period of time for which the interception is required to be maintained. Finally, the affidavit must include information regarding all previous applications made under the law.143

In articulating the necessity for the interception, the government, for instance, must explain why less intrusive "traditional investigative techniques" would not have exposed the crime.144 Many cases involve assertions that the use of undercover informants had been tried, unsuccessfully, or would have been ineffective145 or too dangerous to employ. The government need not use all potential confidential informants or prove that the informants would be completely useless in order to make the necessity showing.146 The government must also indicate why less intrusive electronic means, such as pen registers or trap-and-trace devices, were not used.147

No order to intercept confidential communications under Title III may be approved for longer than is necessary to achieve the objective of the order, and, in any case, not longer than thirty days. Extensions may be obtained by again submitting a new request to a judge to prolong the interception. The law does not limit the number of extensions.148

Title III also, in its current version, allows so-called "roving wiretaps" when it is not possible to specify with particularity the telephone or communications media the suspect will allegedly use in the suspected criminal enterprise.149

The law provides for judicial control also after the wiretap has been undertaken. The prosecutor may be required to submit reports to the judge on the ongoing status of the intercept. 150 The intercepted communications must also be recorded and made available to the judge after the intercept has been completed. They must be kept for ten years, unless a judge orders their destruction. Within ninety days of the filing of an application that was denied, or the termination of the authorized interception, the judge must notify the person's affected of the fact of the order or application, the time of the interception and whether or not conversations were intercepted and recorded. The judge may "in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest

138 State v. Otte, 887 So.2d 1186 (Fla. 2004).
139 Freiwald (2004, 52).
140 Some call Title III warrants, therefore, "super-warrants." Freiwald (2004, 47-48).
141 18 U.S.C. § 2516(1)(2)(3).
142 United States v. Falcone, 505 F.2d 478 (3d Cir. l974).
143 18 U.S.C. § 2518(1)(b).
144 United States v. Kahn, 415 U.S. 143, 153 (1974)
145 United States v. Thompson, 944 F.2d 1331 (7th Cir. 1991).
146 United States v. Canales-Gomez, 358 F.3d 1221 (9th Cir. 2004).
147 United States v. Dumes, 313 F.3d 372 (7th Cir. 2002).
148 18 U.S.C. § 2518(5).
149 18 U.S.C. § 2518(11).
150 18 U.S.C. § 2518(6).

of justice."151 Judges must report the number of requests for wiretaps they have received, how many were granted, or extended, and the competent prosecutor's office is also obligated to keep detailed statistics related to the interception of confidential communications.152

All law enforcement officials involved in executing the wiretap laws are allowed to share the information they have gained in a legal wiretap or bug, with other law enforcement officials for a valid law enforcement purpose.153

1.3.1.2.3 The Execution of Interceptions Under Title III

1.3.1.2.3.1 Covert Entry to Install Listening Devices

Although Title III nowhere mentioned how "bugs," or secret listening devices are to be planted in the house or business of a suspect, the USSC has held that Title III must have envisioned that this would be necessary, and has thus held that it would not violate the 4.Amend. for officers, who had been issued an order under Title III to "bug" a particular space, could secretly enter the space to plant the microphones.154

1.3.1.2.3.2 The Minimization Requirement

All wiretaps authorized by Title III must " be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."155 This command was designed to prevent "rummaging" during wiretaps or bugging operations by preventing the executing officers from listening to conversations obviously not included in the wiretap authorization. The USSC has not interpreted the "minimization" requirement rigidly, however, holding that the statute does not forbid the interception of all non-relevant conversations, but rather instructs the agents to conduct the survillance in such a manner as to "minimize" such interceptions. Much like with searching of computer files, the USSC majority held that, in a complicated conspiracy case where there were a high number of non-relevant calls, "many of the nonpertinent calls may have been very short. Others may have been one-time only calls. Still other calls may have been ambiguous in nature or apparently involved guarded or coded language. In all these circumstances agents can hardly be expected to know that the calls are not pertinent prior to their termination."156

In an unusual interpretation of the minimization requirement, a court order that required an automobile service company to allow the FBI to use the company's in-car wireless emergency communication system to listen to oral conversations in a suspect's car was invalid because the FBI's surveillance completely disabled portions of the communications system which severely hampered emergency capabilities, thus violating the "minimization" requirement.157

1.3.1.2.4 Statistics on Use of Title III

From 1968 to 2011, 44,256 wiretaps were authorized, 14,549 by federal judges and 29,707 by State court judges. In those 43 years, only 32 applications were denied.158

In 2011, 2,732 wiretaps were authorized, 792 by federal judges, the rest by state court judges. 2,189 intercepts were actually installed, 367 in the federal system. The average number of conversations intercepted for each wiretap was 3,716 involving an average of 118 persons. 868 of the 3,716 intercepts were incriminating in nature.159

In 2012, there was a sharp rise to 3,395 wiretaps authorized, 1354 by federal judges and the rest by State judges. 1,932 extensions were granted, 521 by federal judges. 3,292 of the wiretaps were for portable phones and only 14 for personal residences. Only seven were "roving" wiretaps. 2,967 of the wiretaps, around 87%, were in narcotics cases.160

In 2006, at the federal and state levels, four states, California (430 orders), New York (377), New Jersey (189), and Florida (98) accounted for 59 percent of all wiretap orders.161

151 18 U.S.C. § 2518(8)(a,d).
152 18 U.S.C. § 2519.
153 18 U.S.C. § 2517.
154 Dalia v. United States, 441 U.S. 238 (1979).
155 18 U.S.C. § 2518(5).
156 Scott v. United States, 436 U.S. 128 (1978).
157 In re United States for An Order Authorizing Roving Interception of Oral Communications, 349 F.3d 1132 (9th Cir. 2003)
158 http://epic.org/privacy/wiretap/stats/wiretap_stats.html
159 http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table4.pdf
160 http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx
161 Schwartz (2008, 292).

1.3.1.3 The Foreign Intelligence Surveillance Act (FISA)[162]

1.3.1.3.1 History

It has always been recognized in the US that the President may conduct "national security" surveillance without court authorization. Title III even provided that "nothing in this statute shall limit the constitutional power of the President to protect the national security of the US."[163] However the limits between "intelligence" gathering and criminal prosecution became blurred. Since the 1940s the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA) collaborated in a secret domestic intelligence operations and during late 1960s and early. The FBI's investigations extended to prominent members of the women's liberation movement, the Black Power movement and critics of the Vietnam War. Between 1967 and 1970, the US Army conducted wide-ranging surveillance, amassing extensive personal information about a broad group of individuals. In 1970, Congress significantly curtailed the Army's program, and the records of personal information were eventually destroyed.[164]

In 1972, the USSC held that the president did not have power to intercept private conversations in cases of domestic security threats without judicial authorization and basically limited this authority to the surveillance of foreign agents.[165] FISA, which was finally promulgated in 1978, was an attempt to delineate the extent of presidential powers to intercept confidential communications, and basically introduced a warrant requirement where surveillance could affect US citizens or permanent residents.

1.3.1.3.2 The Power of the President to Issue Wiretaps Without Judicial Control

The President of the US, acting through the Attorney General may authorize electronic surveillance without a court order to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that: (a) the electronic surveillance is solely directed at the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers; or (b) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power. There must also be no substantial likelihood that the surveillance will acquire the contents of any communication to which a "US person" is a party.[166]

For the purposes of FISA, a "foreign power" includes not only a foreign government, or an entity under the control of a foreign government, or a foreign-based political organization, but also "a group engaged in international terrorism or activities in preparation thereof" and "an entity not substantially composed of US citizens or residents that is engaged in the "international proliferation of weapons of mass destruction."[167]

For the purposes of FISA, a "US person" refers to US citizens, those admitted for permanent residence ("green card" holders) or US legal entities or non-incorporated associations of which a substantial part are US citizens.[168]

For the purpses of FISA, "foreign intelligence information" refers to information that relates to, and if concerning a US person is necessary to, the ability of the US to protect against military attack, sabotage, international terrorism, the international proliferation of weapons of mass destruction, clandestine intelligence activities, or infrmation that is otherwise necessary for the national defense or the conduct of US foreign affairs.[169]

Similar to Title III, violations of FISA are subject to penal and civil sanctions.[170]

1.3.1.3.3 Judicial Control under FISA

1.3.1.3.3.1 The Foreign Intelligence Surveillance Court: Its Constitution, Powers and Jurisdiction

In general, the President need only seek authorization from a judge if the proposed surveillance measure is aimed at, or may affect the interests of a "US person."[171]

---

162 50 U.S.C. § 1801 et seq.
163 18 U.S.C. § 2511(3).
164 Solove (2002, 1107-08).
165 United States v. United States District Court, 407 U.S. 297 (1972).
166 50 U.S.C. § 1802(a)(1).
167 50 U.S.C. § 1801(a).
168 50 U.S.C. § 1801(i).
169 50 U.S.C. § 1801(e)
170 50 U.S.C. §§ 1809, 1810.
171 50 U.S.C. § 1802(b)

FISA established a special secret court, Foreign Intelligence Surveillance Court (FISC), to receive requests for foreign intelligence surveillance which might include US persons. It consists of 11 federal district court judges appointed by the Chief Justice of the USSC, of whom no fewer than three shall reside within 20 miles of Washington D.C.172 The Chief Justice also selects a three judge FIS Court of Appeal to hear appeals from denials of requests for surveillance by the FISC.173

1.3.1.3.3.2 Requirements of an Affidavit for a FISC Warrant

Every application for a FISC warrant must be approved by the US Attorney General in the federal system, and by an equivalent official in a State system. It must include the identity, if known, of the target of the surveillance, a statement of the facts and circumstances going to show that the target is a foreign power or an agent of a foreign power, and that each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. There must be a statement of the proposed minimization procedures, a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance, and a sworn statement by a national security official that the information sought is "foreign intelligence information" and that a "significant purpose of the surveillance is to obtain foreign intelligence information."

The affidavit must also assert that such information cannot reasonably be obtained by normal investigative techniques, and must list a summary of the facts concerning all previous applications that have been made to any judge under FISA involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application.174

The affidavit may also request the inclusion of provisions to install pen registers and trap and trace devices against the same targets for which the electronic surveillance has been authorized.175

Prior to September 11, 2001 (9-11), the affidavit for a FISA wiretap had to assert that foreign intelligence information was the "primary purpose" of the interception .176 Although one federal court found that this watered-down provision violated the 4.Amend.,177 the new language has been upheld by the federal courts of appeal.178

1.3.1.3.4 Length of Surveillance

Orders for surveillance involving US persons may be approved for the period necessary to achieve its purpose, or for 90 days, whichever is less, while an order targeted against a foreign power, may extend for up to one year, and one targeted against an agent of a foreign power who is not a US person may be for no longer than 120 days. Extensions may be applied for under the same procedures as for the initial order.179

In amendments to FISA in 2008, special provisions were added for the issuance of FISC warrants for the surveillance of US persons living overseas, which may also be authorized for no longer than 90 days.180 The FISC may also issue a joint authorization for surveillance both within and without the US.181

1.3.1.3.5 Minimization Requirements and Other Factors Relating to Execution

"Minimization" procedures under FISA must be adopted by the Attorney General to the end of minimizing the acquisition and retention, and preventing the dissemination of non-publicly available information concerning non-consenting US persons, "consistent with the need of the US to obtain, produce, and disseminate foreign intelligence information. They must prohibit the dissemination of any information about a non-consenting US person "unless such person's identity is necessary to understand foreign intelligence information or assess its importance."182

If the government wants to intercept communications or conduct other FISA-related procedures in relation to foreigners living abroad, they must also engage in procedures to minimize conduct which affects US persons, including targeting a foreigner

172 50 U.S.C. § 1803(a)(1).
173 50 U.S.C. § 1803(b)
174 50 U.S.C. § 1804(a)
175 50 U.S.C. § 1805(i).
176 The language "significant purpose" was added by § 218 US PATRIOT Act in 2001. This broader language was upheld by the FISC Appellate Court in In re Sealed Case No. 02-001, 310 F.3d 717 (USFIS App. 2002).
177 Mayfield v. United States, 504 F.Supp.2d 1023 (D.Ore. 2007).
178 United States v. Duka, 671 F.3d 329 (3d Cir. 2011).
179 50 U.S.C. § 1805(d)(1,2).
180 50 U.S.C. § 1881b(a).
181 50 U.S.C. § 1881d
182 50 U.S.C. § 1801(h)

abroad, where the actual target would be a US person, whether living abroad or in the US. Such surveillance must in general comply with the 4.Amend. The FISC must approve these minimization measures.183

1.3.1.3.6 FISA Statistics

From 1979 through 2008 there were more than 14,000 applications for FISA wiretaps and not one was denied through 2003. Between 1978 and 1995 there were more than 500 applications or extensions per year. After 1995 the yearly number began to rise reaching a peak of 2,181 wiretaps in 2006, only one of which was rejected by the FISC.184 In 2012, the FISA approved all but one of the 1,856 applications submitted to it.185

1.3.1.4 Application of 4.Amend. Doctrine to Wiretapping and Bugging

1.3.1.4.1 The Third Party Consent Doctrine

Title III provides that it is not unlawful for state officials to intercept a confidential communication if a participant in the communication has given prior consent to the interception.186 It is also not unlawful for a citizen, who is not working with law enforcement, to intercept or record a conversation to which it is a party or where one of the parties has given their consent, unless such communication is intercepted for the purpose of committing any crime or civil wrong.187

Most States follow Title III in this respect, and some States even allow children to consent to police eavesdropping.188 Some jurisdictions will also allow parents to "consent" to police overhearing the confidential conversations of their minor children.189 A minority of States require a judicial order even when a participant in a telephone conversation consents, thus giving more protection than federal law.190

Thus, when an arrested person allows a police officer to use his or her phone to exchange text messages with an unwitting criminal confederate, this would not normally fall within the prohibitions of US wiretap statutes.191 Some courts also allow police to answer a call to a lawfully seized cellular telephone, even without the consent of the owner, because the caller sacrificed any reasonable expectation that his call would remain private by not confirming the identity of the person who answered the phone.192

The third party consent doctrine also applies to FISA intercepts.

1.3.1.4.2 Exception for Exigent Circumstances

An order need not be obtained, however, when the prosecutor, otherwise possessing the requisite probable cause required by Title III, determines that an "emergency situation" exists, that involves: (1) immediate danger of death or serious physical injury to any person; (2) conspiratorial activities threatening the national security interest, or (3) conspiratorial activities characteristic of organized crime. When this occurs, the prosecutor must, within 48 hours, get *post facto* authorization from a judge. If this is not obtained, the results of the interception are inadmissible in any legal proceeding as provided by the statutory exclusionary rule discussed in Section 1.2.4.3 below.193

Under FISA, the Attorney General may authorize the emergency employment of electronic surveillance if he/she gets retroactive approval of the FISC within seven days after the surveillance was authorized. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance,

183 50 U.S.C. § 1881a(b).
184 Abrams (2008, 419-20).
185 http://epic.org/privacy/wiretap/stats/fisa_stats.html
186 18 U.S.C. § 2511(2)(c).
187 18 U.S.C. § 2511(2)(d).
188 Malone v. State, 541 S.E.2d 431 (Ga. 2000).
189 Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998); State v. Spencer, 737 N.W.2d 124 (Iowa 2007); State v. Whitner, 732 S.E.2d 861 (S.C. 2012). Some States extend more protection, however, and do not allow parents to give vicarious consent for the overhearing and recording of their children's conversations. See Bishop v. State, 526 S.E.2d 916 (Ga. App. 1999); State v. Christensen, 102 P.3d 789 (Wash. 2004).
190 State v. Allen, 241 P.3d 1045 (Mont. 2010)
191 Commonwealth v. Cruttenden, 58 A.3d 95 (Pa. 2012)
192 State v. Gonzalez, 898 A.2d 149 (Conn. 2006).
193 18 U.S.C. § 2518(7)

the evidence may not be used.194 After a Congressional declaration of war, the President may also authorize interceptions involving US persons for 15 days without a warrant.195

1.3.1.4.3 Exclusionary Rules and other Sanctions for Violations of the Wiretap Laws

Title III empowers any person, whose conversations were overheard to move to suppress their use if (1) the communication was unlawfully intercepted; (2) the order of authorization or approval under which it was intercepted is insufficient on its face; or (3) the interception was not made in conformity with the order of authorization or approval. The same is true for FISA.196

If the motion is granted, the contents of the intercepted communication, or evidence derived therefrom (i.e., the "fruit of the poisonous tree") are inadmissible in court. The prosecutor has a right to appeal a decision suppressing evidence within 30 days of the decision.197

Evidence derived from a wiretap which was not authorized by the federal or state attorney general or authorized delegates must be suppressed.198 Fruits of illegal wiretaps may also not be used to impeach a testifying defendant, as may the fruits of a search made in violation of the 4.Amend.199 Some courts have also held that there is no "good faith" exception to the Title III exclusionary rule, unlike the 4.Amend. exclusionary rule (See below).

However, violations of provisions of Title III that were not "intended to play a central role" in the regulatory scheme, will not necessarily lead to suppression of evidence otherwise legally gathered.200 Examples are violations of the recordation and sealing requirements,201 violation of the notice provision,202 and violation of the minimization requirements.

The 4.Amend. does not require exclusion of evidence gathered illegally by private persons who are not working with the police. This regime is different in relation to wiretaps, however, as a private person may violate Title III by intercepting conversations. The courts, however, are divided as to the extent the government may use evidence gathered through illegal wiretaps or buggings by private persons.

Some courts say that if the government has "clean hands" in the affair, the evidence may be used.203 Some even allow evidence from private hackers whose activities the government has approved of after-the fact.204 Others will allow evidence if the private person inadvertently overhears a conversation.205 Some States will exclude privately gathered evidence by applying State privacy laws and even the fruits gathered lawfully by the police after using the illegally intercepted conversations.206 A minority of federal courts also reject the "clean hands" doctrine and will exclude information gathered through illegal private wiretaps.207

The victim of an unlawful interception of communications in violation of Title III also has a statutory right to bring a civil action against the government and the court may impose administrative sanctions on the government as well.208

If the FISC refuses to approve an emergency wiretap, then no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any US person acquired from such surveillance shall subsequently be used

194 50 U.S.C. § 1805(e)(1). A seven-day emergency period is also allowed for the use of pen registers and trap-and-trace devices. 50 U.S.C. § 1843.
195 50 U.S.C. § 1811. This also applies to pen registers and trap and trace devices. 50 U.S.C. § 1845.
196 18 U.S.C. § 1806(c,e)
197 18 U.S.C. § 2518(10)
198 United States v. Reyna, 218 F.3d 1108 (9th Cir. 2000); State v. Bruce, 287 P.3d 919 (Kan. 2012).
199 People in re. A.W., 982 P.2d 842 (Colo. 1999).
200 United States v. Giordano, 416 U.S. 505 (1974); United States v. Chavez, 416 U.S. 562 (1974)
201 United States v. Amanuel, 615 F.3d 117 (2d Cir. 2010); United States v. Ojeda Rios, 495 U.S. 257 (1990).
202 People v. Rodriguez, 970 N.E.2d 816 (N.Y. 2012); United States v. Donovan, 429 U.S. 413 (1977)
203 United States v. Murdock, 63 F.3d 1391 (6th Cir. 1995).
204 United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003)(a Turkish "unknownuser" case).
205 Adams v. Sumner, 39 F.3d 933 (9th Cir. 1994)(switchboard operator at hotel overhears conversation).
206 State v. Faford, 910 P.2d 447 (Wash. 1996).
207 Chandler v. Simpson, 125 F.3d 1296 (9th Cir. 1997); Berry v. Funk, 146 F.3d 1003 (D.C.Cir. 1998); United States v. Crabtree, 565 F.3d 887 (4th Cir. 2009).
208 18 U.S.C. § 2520

or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.209

When evidence is gathered overseas, the US courts have developed a nuanced approach to whether such evidence can be used in trials taking place in the US in cases not deemed to be covered by FISA. In general, these cases revolve around interpretations of the 4.Amend. When the US participates in the search of a foreigner's residence abroad, then the 4.Amend. is not applicable and the evidence may be used in US courts.210

If the US, however, is involved in a joint investigative operation with a foreign law enforcement agency and the target is a US person, then the 4.Amend. will be applicable. But in a case involving Danish wiretaps of a suspected American drug dealer in Denmark, a federal court held that, if the foreign investigators followed their own laws and they did not radically depart from American practices in a manner that would "shock the conscience," then the evidence would be usable.211 When the 4.Amend. *is* applicable to a search involving an American citizen abroad courts are flexible in relation to the warrant requirement because there is not always an ability to obtain a warrant abroad in such situations.212

When it comes to the interception of electronic communications, their acquisition from storage, the installation of pen registers, etc., the ECPA and the SCA provide for no exclusionary rules. And even if police ignore the minimal requirements for getting a court in these cases, the federal courts has held that there is no provision for suing the officers who wilfully violated the law.213

1.3.2 Government Access to Stored Communications

1.3.2.1 Introduction

The SCA was passed in 1986 to deal with the problems which arose when electronic communications began to replace wire communications. As was mentioned above, it is virtually impossible, without hacking into a computer, to intercept an e-mail message simultaneously with its transmission. E-mail and voice-mail is invariably stored with the internet or telecommunications service provider immediately after it is sent and is then downloaded by the intended recipient.

Thus, in a sense, one has entrusted these conversations to a third party, which under 4.Amend. analysis, might mean there is no reasonable expectation of privacy in their contents. However, one does the same with a posted letter, the contents of which are protected by the 4.Amend. As we will see, the SCA gives these stored communications less protection than Title III does to simultaneously "intercepted" communications, but does not fully deprive them of 4.Amend. protection.

1.3.2.2 The Stored Communications Act (SCA)

For the government to access the content of stored voice-mail or e-mail messages, a search warrant is needed if the communication has been held in storage with the provider for 180 days or less, whereas a subpoena or court order without a showing of probable cause is sufficient if it has been held more than 180 days.214 The standard for such a subpoena or order is that "there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."215

The federal government maintains, however, that the rules change if the recipient has actually accessed a message before the 180 days have elapsed. Once an e-mail is opened, the government maintains, though this is not specified in the law, that it may access the content with a subpoena. 216 There is, however, disagreement among the federal courts on this "open and unopened" communications distinction.217

A Congressional inquiry determined that cellphone carriers responded in 2011 to 1.3 million demands from law enforcement agencies for text messages and other information about subscribers.218

---

209 18 U.S.C. § 1805(e)(5).
210 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).
211 United States v. Barona, 56 F.3d 1087 (9th Cir. 1995).
212 In re Terrorist Bombings of U.S. Embassies in East Africa: US v. Odeh, 552 F.3d 157 (2d. Cir. 2008).
213 Tucker v. Waddell, 83 F.3d 688, 693 (4th Cir. 1996), cited in Freiwald (2004, 59).
214 18 U.S.C. § 2703(a). According to the legislative history, Congress analogized the short-term storage of electronic contents to a safety-deposit box, long-term storage, on the other hand, to business records held by third parties. Freiwald (2004, 50).
215 18 U.S.C. § 2703(d).
216 This interpretation is expressed in US DOJ training materials. Freiwald (2004, 57).
217 Young (2012, 26-27).
218 Sengupta (NYT, 26 Nov 2012)

1.3.2.2.1 Exclusionary Rules and Notice Provisions

Unlike Title III and FISA, the SCA contains no exclusionary rule to deter violations of the statute.219 If the government or the service provider violates the provisions of the SCA, only civil or administrative remedies are available.220 However, where the statute requires a search warrant (for conversations or held less than 180 days), the 4.Amend. applies and exclusion would be the result of a violation.221

Unlike with the wiretap statutes, the SCA also explicitly excuses the government from providing notice to targets whose stored communications have been accessed.222

1.3.3 Government Access to Communications Metadata

1.3.3.1 Introduction

Since the 4.Amend. does not protect communications metadata, such as the telephone numbers involved in confidential communications,223 that is the "external" or "envelope" information regarding communications, the 4.Amend. exclusionary rule plays no role in this area and authorities do not need probable cause to access such information through the use of pen registers, trap and trace devices (for contemporaneous interception), or court orders, subpoenas or other requests for stored records of this information. The rules pertaining to this area are contained, however, in the "Pen Registers Act" section of the ECPA.

1.3.3.2 The Pen Registers Act

A "pen register" is defined as a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A "trap and trace device" is defined as "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication. Both definitions exclude the content of communications. 224

Federal courts have interpreted these definitions to also include the "envelope" data related to e-mail and internet surfing, i.e., the "uniform resource locators (URLs) of websites a person visits, or the e-mail addresses involved in electronic communications. 225 The majority of courts have held that, as with telephone numbers dialed, a person has no reasonable expectation of privacy in the websites they visit.226 Nearly all courts have also held that internet subscriber information is not protected by the 4.Amend. 227

A pen register or trap and trace order can be issued by a federal judge and must state (1) the person in whose name the telephone line to which the device will be attached is listed, (2) the identity of the target of the investigation, (3) the telephone number and physical location of the telephone line to which the device will be attached, and (4) a statement of the offense to which the telephone numbers likely to be obtained relate.228 The pen/trap order is good for 60 days, but may be renewed.229

A pen/trap order may be issued for any crime, unlike a wiretap, and there is no provision to notify those whose communications have been identified by a pen or a trap.230

---

219 18 U.S.C. § 2708.
220 18 U.S.C. §§ 2707, 2712.
221 United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
222 Freiwald (2004, 64-65).
223 See section 1.2.1.3.3. above, citing United States v. New York Telephone Co., 434 U.S. 159 (l977); Smith v. Maryland, 442 U.S. 735 (1979).
224 18 U.S.C. § 3127(3,4).
225 In re Application of the United States for Order Authorizing Installation and Use of Pen Register and Trap & Trace Device on E-Mail Account, 416 F.Supp.2d 13 (D.D.C 2006).
226 Guest v. Leis, 255 F.3d 325 (6th Cir. 2001); United States v. Forrester, 512 F.3d 500 (9th Cir. 2008); State v. Mello, 27 A.3d 771 (N.H. 2011).
227 United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008)(surveying cases); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). Cited in McAllister (2012, 479).
228 18 U.S.C. § 3123(b).
229 18 U.S.C. § 3123(c).
230 18 U.S.C. § 3123(d) prohibits service providers from notifying those whose phones have been targeted.

1.3.3.2.1 Judicial Control of Interception of the Issuance of Pen/Trap Devices

Under the Pen Registers Act, the court makes no independent findings of the basis for the order, but need only find that "the prosecuting officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."231 It is not clear whether courts are even supposed to review pen register applications. In a report, the Senate explained that the "provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted."232

Violations of the Pen Registers Act do not lead to exclusion of the evidence and no provision is made for any civil suits by those whose privacy has been violated. The only sanction is fines and possible imprisonment for a violation.233

A number of States, however, provide more protection than does the 4.Amend and the Pen Register Act and require probable cause or judicial authorization under their statutes.234 Some States also recognize an expectation of privacy under their State constitutions in relation to websites visited.235

The FBI has used special software and hardware called "Carnivore" to collect information from e-mail messages traveling through the e-mail server of an internet service provider, especially if the provider is unwilling to comply with a court order. Carnivore scans the "smallest subset" of information from incoming and outgoing e-mail messages and duplicates it, while letting the stream continue to flow. Extraneous information will remain only temporarily in random access memory and will not be fixed in a stable, recorded format. The FBI maintained already in 2000 that section 18 U.S.C.§ 3121 of the pen register and trap-and-trace law and wiretap law authorize the use of Carnivore.236 Since passage of the Patriot Act in 2001, agents may now install Carnivore by simply obtaining an order from a U.S. or state attorney general — without going to a judge. After-the-fact judicial oversight is still required. Voices in the literature have pointed out that it is incorrect to analogize a telephone number dialed, with modern devices, such a Carnivore, which collect all exterior data associated with the visiting of a website.237

1.3.3.3 Statistics and Transparency

The government is also not obligated to publish each year the number of pen registers or trap and trace devices used, as it is with wiretaps. There is a vague requirement to inform Congress,238 but the figures, when and if conveyed to Congress, are seldom made public. A leak, however, did reveal some data for the years 1999-2003. In 1999, there were 6,502 orders; in 2000, 6,079; in 2001, 5,683; and in 2002, 5,311. Then, there was a dramatic rise in 2003 with 7,258 pen/trap orders. The 2003 amount represents an 11.6 percent increase in federal use of pen/trap orders over the five-year period that began in 1999, and, more dramatically, a 29.9 percent increase from the preceding year. Federal use of wiretaps declined over a similar period between 1999 and 2006.239

1.3.3.4 Exceptions to the Subpoena Requirement for National Security: National Security Letters (NSL)

1.3.3.4.1 Section 215 of the Patriot Act

The federal government's ability to use National Security Letters (NSLs) to force private businesses to turn over records of transactions with citizens, whether it be telephone and e-mail records, financial records, or credit records, without the judicial control required for subpoenas, was greatly expanded by § 215 of the Patriot Act, passed in a hurry after the attacks of 9-11 in October, 2001.240 The Patriot Act amended FISA to authorize not only the seizure of "business records," but also "any tangible thing from any third party record holder (including books, records, papers, documents, and other items," and lowered the standard for gathering such items from the requirement of alleging "specific and articulable facts" relating to terrorist activity to a

231 18 U.S.C. § 3123(a)(1).
232 Freiwald (2004, 62).
233 18 U.S.C. § 3121(d). Apparently, no one has ever been charged under this section. Freiwald (2004, 64-65).
234 State v. Thompson, 760 P.2d 1162 (Idaho 1988); People v. Sporleder, 666 P.2d 135 (Colo. 1983); State v. Rothman, 779 P.2d 1 (Haw. 1989); State v. Hunt, 450 A.2d 952 (N.J. 1982); Commonwealth v. Melilli, 555 A.2d 1254 (Pa. 1989); Richardson v. State, 865 S.W.2d 944 (Tex. Crim. App. 1993); State v. Gunwall, 720 P.2d 808 (Wash. 1986).
235 State v. Reid, 945 A.2d 26 (N.J. 2008). One court said there was a difference between a website, such as that of a newspaper, and an URL, which could reveal which article the person read on the website. Doe v. Prosecutor, Marion County, Indiana, 566 F.Supp.2d 862, 880 (S.D. Ind. 2008), discussed in McAllister (2012, 479-80).
236 69 U.S.L.W. 2053 (2000).
237 Freiwald (2004, 61).
238 18 U.S.C. § 3126.
239 Schwartz (2008, 297).
240 Pub. L. 107-296 (2001). § 215 is now codified in 18 U.S.C. § 2709 of the SCA.

mere assertion that the items are "relevant to the investigation" of terrorism and necessary to "protect against international terrorism or clandestine intelligence activities."

FISA also includes provisions for the issuance of NSL's based on an assertion that "the tangible things sought are relevant to an authorized investigation" under the terms of FISA,241 but they may not be issued for records of US persons for items which would be protected under the First Amendment of the US Constitution protecting freedom of speech and association.242

The law also originally provided that anyone receiving a NSL was prohibited from disclosing "to any other person that the [FBI] has sought or obtained tangible things under this section." After lawsuits challenged the anti-disclosure provision, 243 the law was amended to require the government to assert in relation to a particular NSL that disclosure would endanger national security was deemed to be unappealable.244

1.3.4.4.2 Extent of Use of NSL's

The FBI issued around 8,500 NSL's in 2000, with the number increasing to 39,000 in 2003, 56,000 in 2004 and 47,000 in 2005. The overwhelming majority sought telephone toll billing records, subscriber information (telephone or e-mail) or electronic communication transactional records under the SCA. The reason for the increase was attributed to the lessened suspicion required for issuing the NSL. The FBI claimed the most common use of the NSL's was to support FISA applications for electronic surveillance, physical searches or pen register/trap and trace orders."

NSL's were used to get library and bookstore records, until an uproar from library professionals got that section removed from § 215 in amendments in 2006. It was also used with sellers and rentals of scuba diving equipment when government agents feared terrorists might swim ashore in California to wreak havoc.245

Of the 143,074 NSL's issued from 2003-2005, approximately half concerned U.S. citizens. None of the information obtained by NSLs was required to be destroyed even after the information was determined to concern innocent Americans. During the same period, 34,000 law enforcement and intelligence agents had unrestricted access to phone records collected through NSLs. Subscriber information in relation to11,100 different phone numbers were turned over to the FBI in response to only nine NSLs. Despite the huge amount of information gatheed, the FBI only referred 43 cases to prosecutors, 19 of which involved fraud, 17 immigration violations and 17 money laundering. Only one referral resulted in a terrorism related conviction, for material support. 246

In 2012, the government issued more than 1,850 requests under FISA, and 15,000 NSL's. Between 2008 and 2012, only two of 8,591 applications under FISA were rejected.247

1.3.5 The National Security Agency's Worldwide Electronic Surveillance and Data-Collection Operations

1.3.5.1 The National Security Agency (NSA)

The National Security Agency (NSA) is the largest US intelligence agency with the largest budget. It is responsible for collecting and analyzing foreign intelligence. The Armed Services Security Agency was created in 1949 and was rebaptized as the NSA in 1951. Its headquarters is located in Fort George C. Meade in Maryland, not far from Baltimore.

NSA has is huge new storage center for data, a one million square-foot fortress in the little city of Bluffdale, Utah. Since 2006, NSA employs 15,986 military personnel and 19,335 civilians with a yearly budget of 6,115,000,000 dollars.248 NSA has also created intercept stations across the country and helped build one of the world's fastest computers to crack the codes that protect information.249

1.3.5.2 The NSA's Secret Wiretapping Operations (2001-2008)

In the wake of the 9-11 attacks, President George W. Bush authorized the NSA to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the US and a participant in "the call was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization." This secret practice, which

241 50 U.S.C. § 1861(b)(2)(A).
242 50 U.S.C. § 1861(a)(2)(A).
243 John Doe Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008).
244 50 U.S.C. § 1861(f)(C); 18 U.S.C. § 2709(c)(1).
245 Moss, Fessenden (NYT, 10 Dec 2002).
246 Wells (2012, 132).
247 Miller (NYT, 14 Jun 2013).
248 Poitras et al (2013, 82).
249 Risen, Lichtblau (NYT, 9 Jun 2013).

circumvented FISA, because it involved tapping of US persons, was revealed in 2005 by the New York Times and other newspapers and originally caused an uproar in the the public and in Congress.

In this program, NSA accumulated the phone records of millions of Americans in order to conduct "link analysis," another term for event-driven data mining, to sift through the numbers to find those that fit certain profiles, which would then be cross-checked with other intelligence databases. 250

The secret NSA wiretaps were finally evaluated by the FISC in January of 2007, and the practice earlier conducted without the knowledge of FISC, got its blessing in a secret opinion.251

Congress finally yielded to pressure from the executive branch and enacted the FISA Amendments Act of 2008 which established broader authority for intelligence collection overseas than originally provided in FISA, and creating a new framework for targeting the communications of non-U.S. persons located abroad. Under the new provision, the government is not required to demonstrate probable cause that the target of the electronic surveillance is a foreign power or its agent, nor does it require the government to specify the nature and location of each of the particular facilities or places at which the surveillance will occur.252

Under this new regime, electronic surveillance is freed of FISA constraints if the surveillance is "directed at a person reasonably believed to be located outside of the United States." Thus, this telecommunications surveillance can include communications with a US person as long as the surveillance itself is not "directed at" at that person.253

1.3.5.3. The NSA "Prism" Program and the Revelations of 2013

1.3.5.3.1 "Prism" and Programs Aimed at Collecting Information on Foreigners

In the wake of the revelations made by Edward Snowden to the British newspaper *The Guardian* in June of 2013, officials in the administration of President Barack Obama have admitted that NSA has been secretly collecting information on foreigners overseas for nearly six years. The program is called "Prism," and relies on the nation's largest Internet companies to supply the NSA with information in relation to national security threats. It appears that the surveillance has gone beyond what was done in the administration of George W. Bush. The Internet surveillance program employs NSL's authorized by FISA to collect data from online providers including e-mail, chat services, videos, photos, stored data, file transfers, video conferencing and log-ins. The Prism program grew out of NSA's desire to take advantage of the use of social media in its surveillance programs. Although all three branches of government supported the program in relation to gathering communications metadata, Prism appears to be eavesdropping on the contents of communicatons of foreigners, not just the "envelope" material. The government asserts that "Prism" has been authorized by the FISC and comports with the FISA amendments of 2008, which allow the government to obtain an order from FISC to conduct blanket surveillance of foreigners abroad without individualized warrants even if the interception takes place on American soil. The e-mails and phone of US persons can be swept into the database without an individualized court order when they communicate with people overseas.254

Besides capturing communicatons metadata, the NSA was also using its unlimited powers under FISA to wiretap and bug "foreign agents" to monitor the offices of the European Union (EU), and many embassies and diplomatic missions in New York and Washington, including those of France, Italy, Greece, South Korea and Turkey. The monitoring included wiretaps, bugs, the use of antennas, and even tapping into the EU's computer network and copying everything on computer hard drives. NSA also apparently secretly eavesdropped on the Justus Lipsius building in Brussels, where the EU member nations have offices.255

This program, called "Boundless Informant" intercepts in real time all telephone data going in and out of the countries affected. For instance, every month NSA stores the data from around one-half billion communications from Germany, which amounts to the metadata of around 15 million telephone conversations and 10 million internet connections each day. The program spares the US's "good friends", the United Kingdom, Australia, Canada and New Zealand.256 For example, in March 2013, 97 billion pieces of data were collected worldwide, about 14% from Iran, much from Pakistan, and about 3% from inside the US.257

250 Slobogin (2008, 338-39).
251 Clapper v. Amnesty International, U.S.A., 133 S.Ct. 1138 (2013).
252 50 U.S.C. § 1881a. Clapper, 133 S.Ct. at 1144.
253 Schwartz (2008, 308).
254 Savage et al (NYT, 7 Jun 2013).
255 Castle, Schmitt (NYT 1 Jul 2013).
256 Poitras et al (2013, 77-78).
257 Risen, Lichtblau (NYT, 9 Jun 2013).

1.3.5.3.2 The Gathering of Information on US Persons

The Snowden revelations also confirmed the existence of a seven-year effort by NSA to gather and store meta data relating to telephone calls inside the US in which billions of phone calls of US persons have been gathered and stored.258 Although the Obama administration claims it does its best to minimize the incidental interception of communications and data about US persons when intercepting calls to or from foreigners, critics claim that such information is not only recorded but also stored.259 For instance, the FISC issued a NSL which ordered the service provider Verizon in April, 2013, to turn over all metadata on international calls that went in and out of the US on an ongoing basis.260

In a directive signed by Attorney General Eric H. Holder, Jr., NSA eavesdroppers were advised about how to determine whether a target is a foreigner overseas, and what do do if they inadvertently pick up conversations of Americans, whether at home or abroad. Holder advised that the conversations of US persons could be preserved if NSA agents believe it contains information on a "threat of serious harm to life or property" or sheds light on technical issues like encryption or vulnerability to cyberattacks. Current and former NSA officials acknowledge that "incidental" collection of Americans' communications occurs more often today than in the past because of the proliferation of cellphones and e-mail, which can make it harder to determine a person's identity and location.261

Even before the revelation of the extent of the secret NSA operations by Snowden, the Obama administration revealed it had obtained the metadata of more than 20 telephone lines used by Associated Press journalists, including their home and cell phones to investigate so-called "leaks" of information relating to national security issues. The Obama security state has pursued leakers of secret information much more vigorously than have previous administrations.262

In more than a dozen classified rulings, the FISC has created a secret body of law giving the NSA the power to amass vast collections of data on Americans while pursuing not only terrorism suspects, but also people possibly involved in nuclear proliferation, espionage and cyberattacks, officials say. The rulings, some nearly 100 pages long, reveal that the court has taken on a much more expansive role by regularly assessing broad constitutional questions and establishing important judicial precedents, with almost no public scrutiny.

No longer limited to ruling on wiretaps, the FISC, since the 2008 amendments to FISA, has become the ultimate arbiter on surveillance issues. In one important case, the FISC employed the "special needs" doctrine to validate the collection of enormous volumes of communications metadata without probable cause, reasonable suspicion, or a warrant requirement. To actually access the content of the communications, however, they would have to find a justification for a FISA interception. Thus, one official says, the "huge pond of data" can be created without individualized suspicion based on "special needs" but you have to establish a reason to "stick your pole in and start fishing." An example can be seen in one recent FISC case, where intelligence officials were able to get access to an e-mail attachment sent within the United States because they said they were worried that the e-mail contained evidence relating to Iran's nuclear program because "weapons of mass destruction" are now considered to be "foreign intelligence" within the meaning of FISA.

The FISC has also supported the "Mosaic" theory of evidence, and has indicated that, while individual pieces of data may not appear "relevant" to a terrorism investigation, the total picture that the bits of data create may in fact be relevant. 263 The compliant stance of the FISC in rubber stamping the NSA's massive spy efforts may be attributed to the fact that Chief Justice of the USSC, John Roberts, has appointed 10 of the 11 judges, all of whom were Republican nominees and six of which were former executive department employees, usually federal prosecutors.264

1.3.6 The Co-operation of Communications Service Providers in the Implementation of the Law

1.3.6.1 Duty of Communications Service Providers to Cooperate

1.3.6.1.1 The Communications Assistance for Law Enforcement Act (CALEA)

CALEA, passed in 1994,265 requires telecommunications providers to ensure that their facilities are capable of "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any

258 Savage (NYT, 20 Jun 2013).
259 In late July, 2013, the FISC renewed NSA's authority to continue collecting this metadata related to US calls. Shane (NYT, 20 Jul 2013).
260 Savage, Wyatt (NYT, 6 Jun 2013).
261 Shane (NYT, 21 Jun 2013).
262 Savage, Kaufman (NYT, 14 May 2013).
263 Lichtblau (NYT, 7 Jul 2013).
264 Savage (NYT, 26 Jul 2013).
265 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC §§ 1001-1010.

other communications, all wire and electronic communications" to or from a subscriber, and to access call-identifying information that is reasonably available to the service provider, before, during or immediately after the transmission of a communication. These provisions do not, however, expressly include, in relation to pen registers and trap and trace devices, information that may disclose the physical location of the customer other than what can be determined from the telephone number.266

At one time the government sought to compel telecommunications providers to install a so-called "clipper chip" which would enable the government to decipher encrypted texts, but, following pressure from civil liberties organizations, this idea was shelved and CALEA specifically provides that telecommunications carriers "shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."267

CALEA also requires telecommunications providers to expand their capacity for allowing wiretaps, trap and trace and pen register devices, and other interception modalities to accomodate law enforcement requirements and to inform the government about the capacity they have achieved.268 The government was authorized to reimburse telecommunications carriers for reasonable expenses incurred to accomodate to the demands of CALEA that were incurred before January 1, 1995, but such reimbursement now is discretionary.269

In 2005, the Federal Communications Commission (FCC) extended its interpretation of CALEA and required non-commercial internet providers such as universities, schools and libraries to aid the government in wiretapping and data collection, and extended the duties to Voice over Internet telephone services, such as Vonage and Skype.270.

If a court authorizing an interception or pen/trap order under ECPA, FISA or State statutes, finds that a service provider has failed to comply with the requirements of CALEA, the court may order the server to comply. Compliance may also be effected through a civil action filed by the Attorney General. The court may impose a civil penalty of up to $10,000 per day for each day in violation.271

1.3.6.1.2 Provisions of Other Statutes Requiring Cooperation of Service Providers

Pursuant to Title III, and FISA, communications service providers must provide information, facilities, or technical assistance necessary for law enforcement to intercept wire, oral, or electronic communications or to conduct electronic surveillance, if the service providers have been served with a court order directing such assistance or certification in writing by an authorized prosecutor that no warrant or court order is required by law. No communications service provider may disclose the existence of any interception or surveillance upon penalty of civil damages. No cause of action shall lie in any court against any communications service provider for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification. 272 The service provider will be compensated for reasonable expenses incurred in providing such facilities or assistance.273

1.3.6.1.3 Cooperation of Communications Service Providers with the Secret NSA Surveillance and Data Collection Operation

The revelations in 2005-06 about the NSA's secret program revealed a close co-operation between the NSA and service providers, especially the giant AT & T, which had allosed NSA to attach a "black box" to its incoming cable, enabling it to mine the entire content of information channeled by AT & T.274 AT&T also provided NSA with the telephone calling records of tens of millions of Americans. This eavesdropping went as far as to use computers to actually listen to the content of calls and collect key words, which, if found, would give rise to a more traditional investigation.275 Some service providers fought the FISA amendments legislation in 2008, however, which ended up giving the government and NSA the ability to expand its data mining to the extent as revealed by Edward Snowden in June 2013.276

266 47 U.S.C. § 1002(a)
267 47 U.S.C. § 1002(a)(3).
268 47 U.S.C. § 1003
269 47 U.S.C. § 1008
270 Palfrey (2008, 253).
271 18 U.S.C. § 2522
272 18 U.S.C. § 2511(2)(a); 50 U.S.C. §§ 1802(a)(4); 1805(h).
273 18 U.S.C. § 2518(4); 50 U.S.C. § 1805(c)(2).
274 Palfrey (2008, 244, 254).
275 Schwartz (2008, 307).
276 Miller, Perlroth (NYT, 29 Jun 2013).

Snowden brought the world's attention to the NSA's current "Prism" program, which relies on the nation's largest Internet companies like Google, Facebook, Apple, Yahoo, Microsoft, Paltalk, AOL, Skype and YouTube, to supply the NSA with information in relation to national security threats. While the Snowden revelations indicate that NSA obtained direct access to the companies' servers, several of the companies — including Google, Facebook, Microsoft and Apple — denied that the government could do so.277

Microsoft, despite its denials, has been providing NSA with up-to-date access to its customer data whenever the company changes its encryption and related software technology, especially as it relates to its Outlook and Hot Mail services. It also has provided the FBI with access to its SkyDrive service, a cloud storage service with millions of users. The information collected through the Prism program was shared with the FBI and CIA.278

However, a US expert in surveillance has indicated that the denials of active support by service providers is unimpotant, if NSA actually controls the cables through which all of the service provider's communications flow. NSA actually separates the fiberglass cables and divides them, one goes into the service provider and the other to the NSA control room where filters produced by the Firm Narus and programmed by the NSA commence to filter the massive amounts of information.279 It has been reported, as well, that Verizon had set up a dedicated fiber-optic line running from New Jersey to Quantico, Va., home to a large military base, allowing government officials to gain access to all communications flowing through the carrier's operations center.280

Lawyers working for service providers who handle NSLs, rarely fight in court, as they are not allowed to reveal the existence of the NSL's, but frequently push back privately by negotiating with the government, even if they ultimately have to comply. In addition to Yahoo, which fought disclosures under FISA, other companies, including Google, Twitter and smaller communications providers have challenged the NSL procedures in court. Small companies are more likely to take the government to court, because they have less to lose than the big actors.281

The NSA's relationships with service providers goes further than mere reliance on their facilities. It also engages in aggressive campaigns to lure their most talented cadre to switch allegiances from their private employers to the NSA itself. An example is the chief security officer of Facebook, Max Kelly, who left the social media giant to work for the NSA in 2010. The NSA and private Silicon Valley firms have similar interests, that is, to collect, analyze and exploit large pools of data about millions of Americans. NSA wants access to the data stored by the private firms and is perhaps the biggest customer for data analytics software produced in Silicon Valley. US intelligence agencies have invested in Silicon Valley start-ups also for this purpose. In fact, Paladin Capital Group, a venture capital firm based in Washington, D.C., specializes investing in start-ups that offer high-tech solutions for NSA and other intelligence agencies and its managing director was the director of NSA during the Clinton Administration. Another venture capital company doing the same work as Paladin, is In-Q-Tel, which is financed by the CIA. 282

Service providers are also exploring ways to better help the government in its spying operations. Skype, the Internet-based calling service, began its own secret program, Project Chess, to explore the legal and technical issues in making Skype calls readily available to intelligence agencies and law enforcement officials. Project Chess began about five years ago, before Skype entered the "Prism" program in Feburary 2011 and was ultimately acquired by Microsoft in October 2011. One of the documents about the Prism program made public by Mr. Snowden says Skype joined Prism on Feb. 6, 2011.283

In the first public accounting of its kind, cellphone carriers reported that they responded to a startling 1.3 million demands for subscriber information in 2012 from law enforcement agencies seeking text messages, caller locations and other information in the course of investigations. This constitutes an explosion in cellphone surveillance in the last five years, with the companies turning over records thousands of times a day in response to police emergencies, court orders, law enforcement subpoenas and other requests. The total number of law enforcement requests last year was almost certainly much higher, and the total number of people whose customer information was turned over could be several times higher than the number of requests because a single request often involves multiple callers. For instance, when a police agency asks for a cell tower "dump" for data on subscribers who were near a tower during a certain period of time, it may get back hundreds or even thousands of names.

277 Savage et al (NYT, 7 Jun 2013).
278 Risen (NYT, 12 Jul 2013).
279 Levine (Die Zeit, 20 Jun 2013).
280 Risen, Lichtblau (NYT, 9 Jun 2013).
281 Miller (NYT 14 Jun 2013).
282 Risen, Wingfield (NYT, 20 Jun 2013).
283 Risen, Wingfield (NYT, 20 Jun 2013).

The reports also reveal a sometimes uneasy partnership with law enforcement agencies, with the carriers frequently rejecting demands that they considered legally questionable or unjustified. AT&T alone now responds to an average of more than 700 requests a day, with about 230 of them regarded as emergencies that do not require the normal court orders and subpoena. That is roughly triple the number it fielded in 2007. Sprint reported an average of 1,500 requests per day. There has also been a rise in requests from other providers, with annual increases of between 12% and 16% in the last five years.284

In 2006, phone companies that cooperated in the Bush administration's secret NSA wiretaps in violation of FISA were sued, and were ultimately given immunity by Congress with the backing of the courts. 285 The surging use of cell surveillance was also reflected in the bills the wireless carriers reported sending to law enforcement agencies to cover their costs in some of the tracking operations. AT&T, for one, said it collected $8.3 million last year compared with $2.8 million in 2007, and other carriers reported similar increases in billings.286

Clearly if an ISP has a reputation of secretly divulging information to the government, or even of giving the government access to its encryption software, they will lose business. After the first NSA scandal, Google made public its resistance to a Department of Justice (DOJ) request for a large amount of data on search queries. Other firms, such as AOL, Yahoo!, and Microsoft, complied without a battle in court.287

1.4 Transactional Surveillance and General Access to Records in the Hands of Third Parties

1.4.1 Introduction

Traditional USSC case law stripped citizens of privacy when, due to a service agreement with a bank, telephone company, internet provider, or other business, they turned over otherwise private information to this provider as a condition for receiving the service. Because no 4.Amend. protection is given, a judicial warrant based on probable cause is not required to access this information. Various coercive measures may be used by the government, some involving court participation, such as court orders and subpoenas, others not, such as National Security Letters (NSLs) and informal government "requests." Information from such surveillance and access may be used in an ongoing investigation, or may just be stored in one of the government's many databases and subjected to data mining in the future.

1.4.2 Banking and Financial Transactions

1.4.2.1 Requirement of Subpoena or Search Warrant

Congress has passed legislation prohibiting the government from obtaining records from a financial institution except by subpoena or search warrant.288 The USSC upheld the use of a subpoena to obtain banking records, because it held that the bank customer has no reasonable expectation in the bank's microfilms of checks, deposit slips, and other financial records compiled by the bank.289 These subpoenas are not based on "probable cause," but may be issued if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry."

While subpoenas are also sufficient in New Jersey, that State's more protective constitution requires that the subpoena be issued by a grand jury and allow the customer a period of time to object to the release of the records.290 Other States also gived enhanced protection.291

1.4.2.2 Co-operation Required by Financial Institutions

Banks are required by the Bank Secrecy Act of 1970 (BSA)292 to maintain records of their client's identities, to microfilm certain checks and to keep records of other items. The BSA also authorizes the Secretary of the Treasury to require financial institutions to file reports of certain payments, receipts, or transfers of currency or other monetary instruments, including those in excess of $10,000. These "currency transaction reports" are sent to the Financial Crimes Enforcement Network (FINCEN) which

284 Lichtblau (NYT, 9 Jul 2013).
285 Hepting v. AT&T Corp., 671 F.3d 881 (9th Cir. 2011)(this case involved the secret wiretapping of calls coming in and out of the US in violation of FISA conducted by the administration of George W. Bush).
286 Lichtblau (NYT, 9 Jul 2013).
287 Palfrey (2008, 283).
288 12 U.S.C. § 3410-22.
289 United States v. Miller, 425 U.S. 435 (1976).
290 State v. McAllister, 840 A.2d 967 (N.J. App. 2004).
291 People v. Nesbitt, 938 N.E.2d 600 (Ill.App. 2010); People v. Mason, 989 P.2d 757 (Colo. 1999)(requiring "probable cause" for the issuance of a subpoena.
292 Pub. L. 91-508, 84 Stat. 1114 (1970).

keeps them in computerized storage and makes them accessible to law enforcement.293 These provisions have been upheld by the USSC.294

1.4.3 Government Access to Information from Other Service Providers

Since the USSC does not grant 4.Amend. protection to information given to service providers, the government can access this information without a showing of probable cause. As with bank records or communications metadata, even if the law requires a subpoena, the violation of this law will not usually lead to suppression of evidence gathered in the federal system. Courts have thus found no reasonable expectation of privacy in records of electricity use,295 in pharmacy prescription records, 296 or in medical records from a public health clinic. 297

Some States accord a greater respect for privacy in such records. Thus, the Washington Supreme Court found a violation of its constitutional right to privacy when a public utility turned over records of a suspect's use of electricity without having gotten a court order and held that the evidence could not be used.298 Washington also recognizes an expectation of privacy in one's name in a hotel registry, but would allow access to the information with reasonable suspicion.299 Some courts also require a search warrant for prescription drug records.300

1.4.4 Mail Covers

"Envelope information" is the metaphor used for communications megadata, and, of course, the address and return address one affixes to a letter or package is much more public than an e-mail address or a website one visits. Its its voracious appetite for data, the US government has instited the Mail Isolation Control and Tracking program, in which computers of the US Postal Service photograph the exterior of every piece of paper mail that is processed in the US, about 160 billion pieces, for instance, in 2012. It is not known how long the government saves the images.

Traditionally, criminal investigators would only request "mail covers" on a case by case basis, when one had localized a suspected criminal. The same was true, of course, for wiretaps and pen registers. No judicial control is necessary: all the investigator has to do is to fill out a form to get the information. Mail cover surveillance requests, which are almost always granted by the US Postal Service, are granted for about 30 days, and can be extended for up to 120 days. Requests can be related to criminal activity or national security. Criminal activity requests average 15,000 to 20,000 per year. Officials need probable cause, and a warrant, of course to open a letter.301

1.5 Collecting Information as to Movements and Activities in Public Spaces

1.5.1 Use of Surveillance Cameras and Recognition Technology

Activity in public places or "open fields" is not generally protected by the 4.Amend. It is thus not a "search" within the meaning of the 4.Amend. for police to mount a video camera to secretly record comings and goings in the front yard of a suspect's home,302 or in front of public establishments such as bars.303 Use use of motion-activated video cameras in "open fields" is also permissible without judicial authorization.304 Recording street-corner drug deals, either from a distance by using "bionic ears" and binoculars,305 or by outfitting an informer's automobile with a video camera have not violated State privacy protections.306 Using cameras in semi-public places like hospitals307 or open businesses308 also arouses no 4.Amend. concerns. Once information has been revealed in public, the police then may subject that information to technologically assisted interpretation and evaluation without further implicating the 4.Amend.

---

293 Thaman (2001, 886-88).
294 California Banker's Ass'n v. Shultz, 416 U.S. 21 (1974).
295 People v. Stanley, 86 Cal.Rptr.2d 89 (Cal. App. 1999); State v. Domicz, 907 A.2d 395 (N.J. 2006).
296 State v. Russo, 790 A.2d 1132 (Conn. 2002)
297 State v. Mubita, 188 P.3d 867 (Idaho 2008); Commonwealth v. Efaw, 774 A.2d 735 (Pa. 2001)
298 In re Maxfield, 945 P.2d 196 (Wash. 1997).
299 State v. Jordan, 156 P.3d 893 (Wash. 2007); In re Nichols, 256 P.3d 1131 (Wash. 2001).
300 Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005); State v. Skinner, 10 So.3d 1212 (La.2009).
301 Nixon (NYT, 4 Jul 2013).
302 State v. Holden, 964 P.2d 318 (Utah App. 1998).
303 State v. Augafa, 992 P.2d 723 (Haw. App. 1999)
304 United States v. Vankesteren, 553 F.3d 286 (4th Cir. 2009).
305 Stevenson v. State, 667 So.2d 410 (Fla. App. 1996).
306 State v. Clark, 916 P.2d 384 (Wash. 1996).
307 United States v. Gonzalez, 328 F.3d 543 (9th Cir. 2003).
308 Cowles v. State, 23 P.3d 1168 (Alaska 2001).

There is thus no constitutional impediment to using facial recognition technology in relation to photographs or videotapes of persons in public.

1.5.2 Automatic License Plate Recognition (ALPR) and Warrant Checks

ALPR cameras are used in many jurisdictions. All Oklahoma license plates are now ALPR-compatible. New York State uses the system to catch car thieves and to scan parking lots for visitors who have outstanding warrants. The system is used to stockpile, from each license plate capture, images, dates, times and GPS coordinates which can help place a suspect at a scene, aid in witness identification, pattern recognition or the tracking of individuals. Such data can be used to create specialized databases that can be shared among police departments.309

Police officers may also routinely access a computer to determine whether a particular license plate is associated with prior criminal violations, or whether an arrest warrant has been issued for its owner or regular user. They may do this without stopping the vehicle, or after a valid vehicle stop, where they may directly check the records for the driver or the passsenger.

If the stop of the vehicle was unlawful, then some courts prevent use of the information gained from the warrant check. If a lawful stop, however, is excessively prolonged in order to perform a warrant check, some courts forbid use of the warrant information.310 Other courts, however, allow prolongation for a reasonable time to consummate the warrant check.311

No individualized suspicion is needed to run the name of either a driver or a passenger through the national computer system.312

1.5.3 Use of Tracking Devices

1.5.3.1 The "Beeper" Cases

No 4.Amend. implications arose, traditionally, from police following suspects in public. In a couple of cases, police attached an electronic tracking device, or "beeper," to containers of precursor chemicals used in manufacturing illegal narcotics, and then trailed the purchaser of the containers by activating the "beeper." The USSC found no illegal search or seizure in the act of attaching the "beeper" to the container, because it did not yet belong to the suspect and he therefore had no reasonable expectation of private in its interior. And the Court also deemed that trailing suspects in public did not violate the 4.Amend., because police could have used more traditional methods to do the same surveillance.313

If police, however, use the devices to track location inside of the home, judicial authorization would be needed, because it would be a "search" in violation of a reasonable expectation of privacy.314 Recently, the New York Police's strategy of putting tracking devices in decoy pill bottles to deter pharmacy robberies, was upheld by the courts for the same reason.315

1.5.3.2 The Use of Global Posititioning Systems (GPS) Technology for Tracking

Although lower courts had applied the rationale of the "beeper" cases to the use of GPS technology, a recent decision by the USSC has cast doubt on the continued validity of their earlier approach. In *United States v. Jones*, 316 the USSC held, however, that the 4.Amend. was violated when police attached a GPS device to a suspect's automobile and engaged in a four-week surveillance of the suspect's movements. The majority did not, however, find that judicial authorization was needed for the long-term surveillance, but only that the act of attaching the device to the suspect's property was an unlawful "seizure" and violated the 4.Amend, as the automobile belonged to the suspect at the time the device was attached. Five Justices, however, writing in different opinions, did seem to hint that long-term surveillance might violate the 4.Amend.317

Justice Sotomayor opined:

> "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations...[such as] trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union

309 http://en.wikipedia.org/wiki/Automatic_number_plate_recognition#United_States
310 United States v. Boyce, 351 F.3d 1102 (11th Cir. 2003); United States v. Fernandez, 600 F.3d 56 (1st Cir. 2010); People v. Harris, 886 N.E.2d 947 (Ill. 2008);
311 United States v. Purcell, 236 F.3d 1274 (11th Cir. 2001); State v. Williams, 590 S.E.2d 151 (Ga. App. 2003).
312 State v. Sloane, 939 A.2d 796 (N.J. 2008)
313 United States v. Knotts, 460 U.S. 276 (1983)
314 United States v. Karo, 468 U.S. 705 (1984)
315 Goldstein (NYT, 6 Jun 2013).
316 United States v. Jones, 132 S.Ct. 945 (2012).
317 McAllister (2012, 493).

> meeting, the mosque, synagogue or church, the gay bar and on and on." The Government can store such records and efficiently mine them for information years into the future... And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: such as limited police resources and community hostility..Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society. I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."318

Justice Alito, in another concurring opinion, also questioned whether the old USSC approach to public tracking could still stand in the modern technological era:

> "Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.
>
> Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ("crowdsourcing") the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.
>
> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."319

Some US courts had already adopted the position of Justices Sotomayor and Alito that long-term tracking is not "reasonable" under the 4.Amend. before the *Jones* decision,320 but others have followed their approach after the decision.321 Several states require a warrant before GPS devices may be used.322

1.5.3.3 Cellphone Site Location Tracking

As was noted by Justice Alito, as a cell phone moves, its signals are picked up by different cell phone towers located within close geographic proximity. Precise locations can be determined by analyzing signals from such towers, their strength and the angle of signal reception.323 Courts have generally applied the same rationale in *Knotts* to allow police to secure from a cell phone service the location of a subscriber's phone without requiring a warrant for the purpose of tracking the person's movements.324

---

318 132 S.Ct. at 955-56.

319 132 S.Ct. at 963.

320 United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); State v. Jackson, 76 P.3d 217 (Wash. 2003); People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009); United States v. Maynard, 616 F.3d 544 (D.C.Cir. 2010), aff'd *sub nom* United States v. Jones, 132 S.Ct. 945 (2012).

321 State v. Zahn, 812 N.W.2d 490 (S.D. 2012); State v. Brereton, 826 N.W.2d 369 (Wis. 2013); Commonwealth v. Rousseau, --N.E.2d--, 465 Mass. 372 (June 5, 2013)(not yet reported).

322 See McAllister (2012, 506), with statutory cites from California, Utah, Minnesota, Florida, South Carolina, Oklahoma, Hawaii and Pennsylvania.

323 Casey (2008, 1009).

324 United States v. Forest, 355 F.3d 942 (6th Cir. 2004); Devega v. State, 689 S.E.2d 293 (Ga. 2010); In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government, 620 F.3d 304 (3d Cir. 2010).

Service providers maintain records of cellphone site location information (CSLI). Historic CSLI refers to the records maintained by providers that list the cell sites with which a subscriber's cell phone communicated at previous points in time, whereas prospective CSLI refers to the cell sites that a subscriber's cell phone will communicate with at a future point in time. Under the SCA law enforcement agencies may compel service providers to disclose prospective or historic CSLI for a particular cell phone in the course of a criminal investigation.325

The government began to use simple pen register orders, which do not require probable cause, not only to gain access to numbers called, but also to track the location of the cellphone user. In 2005, however, a federal judge rejected the government's application to track the cellphone location of a suspect, claiming that the authorities needed a normal search warrant based on probable cause due to the increased interference with privacy.326 This decision was followed by fifteen "pen register" decisions in other lower federal courts. In eleven of these cases, the courts have refused to issue the order and in four, they have allowed gathering the cell-site information. The government appealed none of these decisions. One New York State court has itself issued contradictory decisions. One panel required "probable cause" for disclosure of historic CSLI,327 whereas the other required only "reasonable grounds" for the discovery of prospective CSLI, which involved monitoring future movements of the suspect.328 On the other hand, the federal district court in Maryland has indicated that historic CSLI is not protected by the 4.Amend. because the defendants in that case "voluntarily transmitted signals to cellular towers in order for their calls to be connected," and the service provider "then created internal records of that data for its own business purposes." 329

The trend appears to be in the direction of requiring a probable cause warrant to disclose this cellsite location.330

Bills have been proposed in the US Congress and in Delaware, Maryland and Oklahoma that would require police to obtain judicial authorization before demanding location records from cellphone carriers and California passed such a law, but it was vetoed by the Governor.331

Sophisticated new technology has now given the NSA the ability to track the activities and movements of people almost anywhere in the world without actually watching them or listening to their conversations. When separate streams of data are integrated into large databases — matching, for example, time and location data from cellphones with credit card purchases or E-ZPass use — intelligence analysts are given a mosaic of a person's life that would never be available from simply listening to their conversations. Just four data points about the location and time of a mobile phone call make it possible to identify the caller 95 % of the time. Intelligence and law enforcement agencies also use a new technology, known as trilaterization, that allows tracking of an individual's location, moment to moment. The data, obtained from cellphone towers, can track the altitude of a person, down to the specific floor in a building.332

1.5.4 The Use of Drones

1.5.4.1 Civilian Use of Drones

Drones can record video images and produce heat maps. They can track fleeing criminals, or political protesters. The Department of Homeland Security (DHS) has offered grants to help local law enforcement buy Drones. Drone manufacturers began to market small, lightweight devices specifically for policing. They are already used to monitor movement on the US borders and by a handful of police departments. Drones for civilian-use are not armed and run on relatively small batteries and fly short distances. In principle, various sensors, including cameras, can be attached to them.

Citizens and civil rights organizations, however, are wary of them and Charlottesville, Virigina, became the first city to restrict their use in February of 2013, and enacted a rule excluding any evidence obtained from a drone. Public protests led the Seattle Police Department to return its two unused Drones. The federal Congress also introduced a bill in February of 2013 prohibiting the use of Drones for targeted surveillance of individuals or property without judicial authorization. In early February of 2013,

325 18 U.S.C. §§ 2701-12. See discussion in Fox (2012, 771).
326 In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. & Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005).
327 Fox (2012, 783).
328 Ibid, citing In re Application of the U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008).
329 United States v. Graham, 846 F.Supp.2d 384 (D.Md. 2012). This is the majority approach. McAllister (2012, 518-20).
330 Casey (2008, 2010, 2016). For cases requiring a warrant and probable cause, see In re Application of the United States, 809 F.Supp.2d 113 (E.D.N.Y. 2011); In re Application of the United States, 747 F.Supp.2d 827 (S.D. Tex. 2010); In re Application of the United States, 736 F. Supp. 2d 578 (E.D.N.Y. 2010), cited in McAllister (2012, 520).
331 Sengupta (NYT, 26 Nov 2012).
332 Risen, Lichtblau (NYT, 9 Jun 2013).

Virginia passed a two-year moratorium on the use of drones in criminal investigations. In several states, including Arizona and Montana, proposals would require the police to obtain a search warrant before collecting evidence with a drone.333

1.5.4.2 Use of Drones for Targeted Killings

Un-manned surveillance aircraft or "Drones" have been used by the CIA and the US Army to assassinate upwards of 3,000 alleged terrorists in Afghanistan, Pakistan, Yemen and Somalia, and in doing so, have caused considerable collateral casualties.334 The Drone strikes have also killed four Americans, including Anwar al-Awlaki.335

The decision as to who is put on the "kill lists" is made secretly within the executive branch of government. In relation to the CIA killings, CIA Director John Brennan is the principal coordinator of the "kill list" with and President Obama allegedly signs off on each person designated for assassination. While the program has eliminated some high Al Qaeda leaders, it now appears to be focusing on lower level cadre, many of whom could have probably been arrested and subjected to a civilian or military trial.336

Uproar over this highly suspect use of Drones has led Congress to discuss whether a new secret court, like the FISC, should be established to decide on which persons should be targed for execution.337 A judge hearing a civil suit brought by relatives of the slain Americans strongly intimated that courts should have a role in the decisions leading to the strikes.338

1.6 Collecting Information as to Activities in Homes and Other Private Spaces

1.6.1 Use of Thermal Imagery and Its Extension to Other Technologies

Thermal imaging technology is based on the electronic capture and imaging of a target's radiated or reflected energy in the thermal portion of the electromagnetic spectrum. It collects and visualizes the thermal energy emitted from all objects by collecting infrared light and focusing it with a lens onto a series of mirrors that direct it onto a detector. The detector then translates the light into an electronic signal that can be displayed on a screen, or amplified, processed, and stored on videotape to be used later as evidence. This technology, the wartime use of which was to detect, for instance, the presence of North Vietnamese or Viet Cong soldiers in the jungles of South Vietnam, is now mainly used to detect excessive use of electricity in homes, symptomatic of the in-door production of marijuana using high power lamps.

Most courts found that training this technology on a house was not a "search" within the 4.Amend, because there was no penetration of the house, and because the energy radiated was seen to be similar to waste or "garbage," without constitutional protection, or because the detection of energy use was like a *sui generis* search that did not otherwise disturb the privacy of the occupants of houses. This approach changed, however, when the USSC held in 2001, that the use of any technology that reveals anything inside the house, even as mundane as the amount of energy used, is protected by the 4.Amend., because "all details are intimate detals, because the entire area is held safe from prying government eyes."339

The *Kyllo* decision would seem to indicate, that a search warrant under the 4.Amend. based on "probable cause" would be required to train a thermal imager on a house. Some courts, however, have engaged in "reasonableness clause balancing" and held that only "reasonable suspicion" was necessary due to the minimal extent of the intrusion.340

In March of 2013, the USSC also held that the use of the "canine sniff," which it had held did not constitute a "search" if trained on a suitcase or a car, or even a person, would constitute a "search" under the 4.Amend. if trained on a dwelling.341

Even before *Jardines*, some courts had held that a canine sniff of a dwelling did constitute a search, and had to be based on probable cause and a warrant.342 Others had engaged in reasonableness clause balancing and held that reasonable suspicion was sufficient to conduct such an investigative measure because the main reason for such searches was to gather evidence which would eventually constitute "probable cause" for the issuance of a search warrant.343

---

333 Sengupta (NYT,16 Feb 2013).
334 Shane (NYT, 8 Apr 2013).
335 Savage, Baker (NYT, 23 May 2013).
336 Worth et al (NYT, 6 Feb 2013).
337 Shane (NYT, 9 Feb 2013).
338 Shane (NYT, 20 Jul 2013, A8).
339 Kyllo v. United States, 533 U.S. 27 (2001).
340 United States v. Kattaria, 503 F.3d 703 (8th Cir. 2007).
341 Florida v. Jardines, 133 S.Ct. 1409 (2013).
342 United States v. Thomas, 757 F.2d 1359 (2d Cir. 1985); State v. Young, 867 P.2d 593 (Wash. 1994);
343 State v. Ortiz, 600 N.W.2d 805 (Neb. 1999); State v. Davis, 732 N.W.2d 173 (Minn. 2007). Some courts even require reasonable suspicion for the canine sniff of an automobile, State v. Wiegand, 645 N.W.2d 125 (Minn. 2005); State v. Tackitt, 67 P.3d 295 (Mont. 2003); People v. Devone, 931 N.E.2d 70 (N.Y. 2010).

1.6.2 Hacking into Computers Located in the Home with Viruses or Other Technology

Commentators speculated that a "perfect computer search" might be possible, if a program could be created that would only find digital contraband, say, in the form of a clearly illegal photograph constituting child pornography. Under the *sui generis* doctrine, no probable cause or even a warrant would be necessary, hypothetically, to conduct such a programmed search.344 After the decisions in *Kyllo* and *Jardines* this would no longer hold if the computer containing the contraband was located in a home.

Already in 2001 it was reported that the FBI was developing software capable of inserting a computer virus onto a suspect's computer and obtaining encryption keys. The software, known as "Magic Lantern," enables agents to read data that had been scrambled, a tactic often employed by criminals to hide information and evade law enforcement. The use of "Carnivore," discussed in section 3.3.3.2.1, above, had proved useless against suspects clever enough to encrypt their files.

Magic lantern installs so-called "keylogging" software on a suspect's machine that is capable of capturing keystrokes typed on a computer. By tracking exactly what a suspect types, critical encryption key information can be gathered, and then transmitted back to the FBI. The virus can be sent to the suspect via e-mail, perhaps through a trusting friend or relative. The virus then watches for a suspect to start a popular encryption program. It then logs the passphrase used to start the program, essentially giving agents access to keys needed to decrypt files.345

Before *Kyllo* and *Jardines,* a court held that federal agents did not violate either the 4.Amend. or the wiretap statute by obtaining a search warrant which authorized the installation of "magic lantern" key logger device on a defendant's personal computer and using the device to discover the passphrase to an encrypted file.346

There are three main approaches to remote searches of computers through the use of "Trojan Horse" or "Magic Lantern"-type technologies. 22 States and federal law require a search warrant based on normal 4.Amend. principles, including exceptions such as that for "exigent circumstances." Twelve States require a search warrant, but have standards which offer more privacy protection than does the 4.Amend. Finally, 16 States prohibit all remote computer searches.347

1.6.3 Secretly Entering a Home or Office to Access Computers

Even before 9-11, federal courts authorized so-called "sneak and peek" warrants, that is, warrants that authorized law enforcement authorities to secretly enter dwellings and other private spaces to gather information relating to future or ongoing criminal activity, often by accessing computers.348

"Sneak and peek" warrants were codified with the passage of the US PATRIOT Act in October, 2001, which amended the law349 to allow a delay in notifying the party whose premises were searched for a "reasonable time" where immediate notice would have an "adverse result."An "adverse result" can include: (1) endangering the life or physical safety of an individual, (2) flight from prosecution, (3) destruction of or tampering with evidence, (4) intimidation of potential witnesses, or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.350 Such "sneak and peek" searches are also allowed, upon warrant issued by the FISC, subject to similar conditions as required for FISA wiretaps.351 US persons who have been the subject of a search under the FISA provisions will only be notified of the search when "the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search."352

From April 2003 to January 2005, the federal government used "sneak and peek" warrants 108 times, an average of 5 warrants per month, which was a sharp increase from 47 warrants between October 2001 to April 2003, i.e., fewer than 3 a month. The DOJ claimed they were used in less than .2% of searches. 353

1.6.4 Warrants to Seize and Search Computers in the Home

1.6.4.1 Introduction

One clearly needs a search warrant, based on probable cause, to enter a house and to seize a computer. A second issue is whether one needs a second search warrant, also based on probable cause, designating what is looked for and copied on the

344 Adler (1996, 1098).
345 Sullivan (2001).
346 United States v. Scarfo, 180 F.Supp.2d 572 (D.N.J. 2001).
347 Brenner (2012, 54).
348 United States v. Villegas, 899 F.2d 1324 (2d Cir. 1990). United States v. Heatley, 41 F.Supp.2d 284 (S.D.N.Y. 1999).
349 § 213 U.S. PATRIOT Act; 18 U.S.C. § 3103a
350 18 U.S.C. § 2705(a)(2).
351 50 U.S.C. §§ 1822-24.
352 50 U.S.C. § 1825(b).
353 Lichtblau (NYT, 5 Apr 2005).

computer's hard drive or other computer storage hardware. Courts routinely hold that a warrant to search for information located on a computer allows executors thereof to seize the computer and conduct a thorough search of all files on the compute so as to separate relevant files from unrelated files.354

1.6.4.2 Probable Cause that Illegal Files Will be Found on a Computer

Law enforcement investigators will often note a specific internet account or internet protocol of a person accessing a child pornography website, subpoena the service provider to determine the address associated with the account, and then seek a search warrant for the home computer at that address. Visiting or becoming a member of such a website is usually enough to constitute probable cause to issue a search warrant for a home computer.355 Other courts, however, require more evidence.356 Some courts have also held that the physical possession of images of child pornography provide probable cause that the person's home computer will also contain such images.357

1.6.4.3 Specificity of a Warrant for Computer Files

Courts generally require a search warrant to search files on a seized computer, unless some exception to the warrant requirement (like search incident to arrest or consent) exists.358 As with the search of a lawyer's office, the search warrant must particularize which of the numerous files on a computer may be copied from the computer hard drive.

Thus, a search warrant that authorized police officers to seize "any and all computer software and hardware, computer disks, disk drives and any and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct" was sufficient not only to seize the computer, but also to conduct an off-site search of files the defendant had previously deleted.359

Sometimes, courts will save an overbroad warrant on the argument that the business searched was "permeated with fraud." This argument was used to justify a brief, warrantless seizure of computers in one case.360 But in a case, alleging a business "permeated by fraud" the warrant, which authorized a search for "evidence of crimes that includes but is not limited to, records and documents, contracts, or correspondence, computer hardware, software ,passwords, telephone toll records, all fax machines, all telephone answering machine, cassettes, typewriter ribbons, phone numbers contained in the memory of an automatic telephone dialer, and caller ID box," was held to violate the 4.Amend. specificity requirement because it could have been more precise.361

If probable cause does exist, but the warrant itself does not particularly describe the place to be searched or the things to be seized, or there is a mistake on the warrant, courts may choose not to exclude the evidence based on the "good faith" rule.362 The "good faith" exception has also been applied to search warrants that are "overbroad" in not sufficiently limiting the officers' discretion as to which documents or files they may open and read.

Thus, a warrant that allowed seizure of "all business records, files, papers, computer hard drives and discs, correspondence and other material constituting evidence of immigration fraud" was held to be overbroad in terms of the 4.Amend., but sufficiently particular for federal agents to have relied in "good faith" on its validity, thus allowing the evidence to be used at trial.363

One federal appeals court held that a search warrant authorizing the wholesale seizure of computer storage media for later off-site examination by law enforcement officers was overly broad absent a supporting affidavit giving a reasonable explanation as to why such a blanket seizure is necessary. Nevertheless, the court applied the "good faith" exception.364

---

354 Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).
355 United States v. Kennedy, 81 F.Supp.2d 1103, 1110 (D.Kan. 2000); United States v. Hambrick, 55 F.Supp.2d 504, 508 (W.D.Va. 1999); United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008), cited in Kerr (2010, 1026-27). United States v. Martin, 426 F.3d 68 (2d Cir. 2005); United States v. Gourde, 440 F.3d 1065 (9th Cir. 2006); United States v. Wagers, 452 F.3d 534 (6th Cir. 2006); United States v. Shields, 458 F.3d 269 (3d Cir. 2006); United States v. Frechette, 583 F.3d 374 (6th Cir. 2009).
356 Another panel of the Second Circuit strongly disagreed with the *Martin* decision (fn. 354) but felt it had to upheld a similar case due to *stare decisis*. United States v. Coreas, 419 F.3d 151 (2d. Cir. 2005).
357 United States v. McArthur, 573 F.3d 608 (8th Cir. 2009).
358 State v. Rupnick, 125 P.3d 541 (Kan. 2005)
359 United States v. Upham, 168 F.3d 532 (1st Cir. 1999)
360 United States v. Bradley, 644 F.3d 1213 (11th Cir. 2011).
361 United States v. Bridges, 344 F.3d 1010 (9th Cir. 2003).
362 Massachusetts v. Sheppard, 468 U.S. 981 (1984). See section 1.2.3.2.3 above.
363 United States v. Kouzmine, 921 F.Supp. 1131 (S.D.N.Y. 1996).
364 United States v. Hill, 459 F.3d 966 (9th Cir. 2006).

1.6.4.4 Overbroad Execution of a Computer Search

It is first fairly typical, that police will make a complete "read-only" copy of a seized hard-drive of the suspect computer. Government agents will then search this copy for the files indicated in the search warrant.365

The USSC has approved of searchers briefly examining each file in the office of a lawyer suspected of real estate fraud, to see if it belongs to the category of files subject to seizure according to the warrant.366 Some courts apply this broad approach to a search of a computer.367 One court noted:"Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer."368

A minority of courts, however, require special search protocols to limit the exploratory nature of searches of computerized material.

Sometimes an authorized computer search for business records will come upon, for instance, files with jpg. suffixes, usually indicating photographs. A narrow approach to computer searches might say the opening of such a "photo" file would be beyond the scope of the warrant.369 If the photo file has a tag that seems to indicate possible child pornography, then the "plain view" doctrine might apply.370 Some courts have approved broad applications of the 4.Amend.'s plain-view doctrine to uphold sweeping searches of suspects' personal computers.371

On the other hand, one federal court of appeal has issued a directive that the government may no longer simply rely on the plain view doctrine in cases in which the investigators rely on the intermingling of computerized records to justify a broad seizure and examination of electronically stored records.372

Where a search warrant authorizes the seizure of certain "documents" or "written material" some courts will allow law enforcement to seize computers as "containers of written documents."373 Othere courts will find the seizure of a computer to be beyond the scope of the search unless the affidavit for the warrant specifically mentions computers, because of the particularly intrusive nature of computer searches.374

1.6.4.5 Third Party Consent as Applied to Computers

No search warrant is needed, of course, if the owner of the computer consents to have the computer seized and searched. Unqualified consent to search premises has been held to extend also to computers found therein.375 Criminal investigators may also rely on the consent of co-owners, or even co-users of a computer to conduct a search without the need to secure judicial authorization. Police thus legally searched the hard drive of a company executive's office computer pursuant to the consent provided by his company's chief financial officer.376

The doctrine of "apparent consent" may also be relied on. Thus in one case, police relied on the apparent authority of the suspect's father to consent to the search of the son's computer, and even did not require police to inquire into whether the computer files were password-protected.377

But, as with other spaces searched pursuant to consent, the police may not exceed the scope of the consent obtained. Thus, if police only obtained consent to search a computer for viruses and other evidence of bank fraud, they could not look for child

---

365 Kimel (2013, 962).
366 Andresen v. Maryland, 427 U.S. 463 (1976).
367 United States v. Richards, 659 F.3d 527 (6th Cir. 2011); U.S. v. Giberson, 527 F.3d 882 (9th Cir. 2008); United States v. Christie, 717 F.3d 1156 (10th Cir. 2013).
368 Unitred States v. Hill, 459 F.3d 966 (9th Cir. 2006); Cf. United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006)("The government should not be required to trust the suspect's self-labeling when executing a warrant."
369 United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) took this approach.
370 Frasier v. State, 794 N.E.2d 449 (Ind. App. 2003). See section 1.2.2.1.3 on the "plain view" doctrine.
See section 1.2.2.1.3 above.
371 United States v. Mann, 592 F.3d 779 (7th Cir. 2010); United States v. Williams, 592 F.3d 511(4th Cir. 2010).
372 United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).
373 People v. Gall, 30 P.3d 145 (Colo. 2011).
374 United States v. Paxton, 573 F.3d 859 (9th Cir. 2009).
375 United States v. Al-Marri, 230 F.Supp.2d 535 (S.D.N.Y. 2002); United States v. Lucas, 640 F.3d 168 (6th Cir. 2011)(consented to search of house or narcotics and "records" related to narcotics sale).
376 United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).
377 United States v. Andrus, 483 F.3d 711 (10th Cir. 2007).

pornography in image files.378 Consent to search a premises for a person, for instances, could not be extended to searching a computer in the house.379 But unrestricted consent to search a car has been held to extend to the seizing of pagers and the calling up of messages stored thereon.380

At least one court has refused to apply the rule of *Georgia v. Randolph*,381 to a situation where one computer user refuses to let police search the computer in the presence of another user.382

1.6.4.6 Encryption and Compelled Divulgation of Encryption Technology

When law enforcement authorities seek to compel a suspect to turn over encryption technology so as to be able to decipher encrypted files, concerns protected by the Fifth Amendment (5.Amend.) of the US Constitution, which prohibits the state from compelling anyone in a criminal case to be a witness against himself, arise.

Analysis of this issue is often based on a USSC case which dealt with state compulsion of a suspect to sign forms directing any foreign banks in which he had accounts to turn records over to a grand jury investigating fraud. The "consent order," which was phrased so as to not constitute an admission that any accounts existed, or to name the banks, was held to not violate the 5.Amend. The court said that the compulsion in this case was more like "being forced to surrender a key to a strong box containing incriminating documents" than to "being compelled to reveal the combination to petitioner's wall safe," the latter of which would be "testimonial" and require the suspect to "disclose the contents of his own mind," which would implicate the protection against self-incrimination according to the case law of the USSC.383

Normally, if the government subpoenas business records with self-incriminating contents, the defendant may not claim the 5.Amend privilege against self-incrimination in relation to the contents of those papers, because the government did not compel him/her to create their self-incriminating contents. But the defendant may claim the 5.Amend. to resist turning over the papers, if the act of turning them over would be "testimonial," i.e., would aid the government in proving either that the documents exist, that they are authentic, or that they are in the possession of the defendant.384 In addition, when the subpoena requires the defendant to search through numerous documents and match them to the one's allegedly in his possession according to the subpoena, the USSC has indicated that this identification process would require the defendant to "use the contents of his mind" in identifying the documents, which would be tantamount to answering a series of interrogatories in a deposition.385

A person may not, however, resist a document or records subpoena, on the above-mentioned grounds, if his or her possession of the document or records is a "foregone conclusion" in the sense that response to the subpoena would not provide the government any information that it did not already have. The "foregone conclusion" doctrine would apply to most corporate records which corporations are required by law keep.386

In one case, a grand jury subpoenaed a defendant in a child pornography case and sought to compel him under oath to reveal the passwords to all of his computers. The court cited the *Doe* case and held that this would violate the 5.Amend, as the grand jury was not seeking documents or objects, but testimony in the form of the passwords, thus equating the passwords more to "combinations" than the "key" to a safe. 387 Similar decisions have been reached in child pornography cases where the grand jury had sought to compel the defendant to produce and decrypt his computer hard drives.388

Several lower federal courts have required a suspect to produce and to decrypt computer files, and have used the "foregone conclusion" exception as a basis for its decision.389 In one case, the FBI, as part of a mortgage fraud investigation, executed a search warrant at defendant's home and seized, among a number of computers, an encrypted laptop found in the defendant's bedroom along with indications that she used it. A court order to compel her to "to produce the unencrypted contents of the

378 People v. Prinzing, 907 N.E.2d 87 (Ill. App. 2009).
379 United States v. Turner, 169 F.3d 84 (1st Cir. 1999).
380 United States v. Reyes, 922 F.Supp. 818 (S.D.N.Y. 1996).
381 547 U.S. 103 (2006). See section 1.2.2.1.5 above.
382 United States v. King, 604 F.3d 125 (3d Cir. 2010).
383 Doe v. United States, 487 U.S. 201 (1988).
384 Fisher v. United States, 425 U.S. 391 (1976); United States v. Doe, 465 U.S. 605 (1984).
385 United States v. Hubbell, 530 U.S. 27 (2000).
386 Fisher v. United States, 425 U.S. 391 (1976); United States v. Doe, 465 U.S. 605 (1984).
387 United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010), discussed in Bales (2012, 1302).
388 In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346, 1352-53 (11th Cir. 2012), cited in Bales (2012, 1302-03).
389 Engel (2012, 563-66).

computer" and the encryption keys was held not to violate her 5.Amend. privilege against self-incrimination, because of the "foregone conclusion" that she was the primary user of the computer. 390

It becomes immeasurably more difficult for government to compel a suspect to give up the password or the encryption tools for suspect files, if the encrypted files are not on the suspect's own computer hard-drives, but are stored in the files of an ICT provider somewhere far away from the defendant's computer, or as some call it, in the "cloud." An encrypted file stored in the cloud will often be very difficult to trace back to an individual, whether because of technical issues or because the file locations are shared among many individuals. This means that the act of producing a password or encryption key, whether it is solely in the suspect's mind or on a written document, will implicitly communicate that the person with the password or key has access to or possession of the electronic files.391

In reality, however, it appears that the government is seldom impeded in its investigations by encryption software, as very few criminal suspects, at least as of 2006, made use of it.392

1.6.5 Use of Informants to Electronically Surveil Activities in the Home

Since the string of decisions ending with *United States v. White*,393 conversations in homes may be surveilled by police without a warrant, if the police can manage to get their wired informant accepted as a guest in the suspect's home or private space, i.e., has "assumed the risk" of communicating with him or in his presence. 394 Using a wired informer has even been allowed when the informer did not speak the language, nor understand the contents of the recorded conversation. 395

The *White* case inspired, however, a strong dissent by Justice Harlan, who questioned whether "we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement." Justice Douglas, also dissenting in *White*, called electronic surveillance "the greatest leveler of human privacy ever known" which penetrates "all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on." He said that "[m]onitoring, if prevalent, kills free discourse and spontaneous utterances. Free discourse--a First Amendment value--may be frivolous or serious, humble or defiant, reactionary or revolutionary, profane or in good taste; but it is not free if there is surveillance. Free discourse liberates the spirit, though it may produce only froth. The individual must keep some facts concerning his thoughts within a small zone of people. At the same time he must be free to pour out his woes or inspirations or dreams to others. He remains the sole judge as to what must be said and what must remain unspoken. This is the essence of the idea of privacy implicit in the First and Fifth Amendments, as well as in the Fourth."396

Several States have followed the dissents in *White* and required police to secure a judicial warrant before sending a wired informant into a dwelling,397 or at least the approval of a high-level prosecutor.398

Some federal courts allow the secret installation of audio or video monitoring devices in a suspect's private dwelling without a warrant if the police have an informant present in the house during the surveilled conversation or activities.399 Other federal courts would, however, require judicial authorization under Title III (the wiretap statute) in such a situation.400

The prevailing view, however, is that warrantless, surreptitious videotaping inside a home by a person who has been invited into the residence does not violate the 4.Amend.401 If government authorities cannot gain consensual entrance into a home to use secret recording devices or videocameras, then they must obtain judicial authorization which follows the guidelines set out in Title III, the wiretap statute.

---

390 United States v. Fricosu, 84 F.Supp.2d 1232 (D. Colo. 2012), discussed in Engel (2012, 563-66).
391 Engel (2012, 568-69).
392 Schwartz (2008, 293).
393 United States v. White, 401 U.S. 745 (1971); See Section 1.2.1.3.2, above.
394 See, for instance, Almada v. State, 994 P.2d 299 (Wyo. 1999).
395 United States v. Longoria, 177 F.3d 1179 (10th Cir. 1999).
396 United States v. White, 401 U.S. at 762-3, Douglas dissenting; 401 U.S. at 786, Harlan disssenting.
397 People v. Beavers, 227 N.W.2d 511 (Mich. 1975); State v. Glass, 583 P.2d 872 (Alaska 1978); Commonwealth v. Brion, 652 A.2d 287 (Pa. 1995); State v. Bridges, 925 P.2d 357 (Haw. 1997); State v. Geraw, 795 A.2d 1219 (Vt. 2002); State v. Mullens, 650 S.E.2d 169 (W.Va. 2007). This includes the "curtilage" in Pennsylvania. Commonwealth v. Bender, 811 A.2d 1016 (Pa. Super. 2002).
398 State v. Worthy, 661 A.2d 1244 (N.J. 1995)(based on reasonable suspicion).
399 United States v. Yonn, 702 F.2d 1341 (11th Cir. 1983); United States v. Myers, 692 F.2d 823 (2d Cir. 1982); United States v. Lee, 359 F.3d 194 (3d Cir. 2004).
400 United States v. Padilla, 520 F.2d 526 (1st Cir. 1975).
401 United States v. Davis, 326 F.3d 361 (2d Cir. 2003); United States v. Wahchumwah, 704 F.3d 606 (9th Cir. 2012).

1.6.6 Video Surveillance in the Home

Although secret videotaping in a home or other private space is not covered in Title III, nor considered to be an "interception" under that statute,402 federal courts in their case law have created requirement of a "super warrant" which closely tracks the requirements of Title III, including the 30 day-limit.403 Video surveillance in the home is also, according to one court, only permissible for a crime that could be the subject of a wiretap under Title III.404

1.7 Access to Electronically Stored Information in Private Possession in General

1.7.1 Accessing Portable I-Phones, Pagers and Other Portable Electronic Storage Devices

As was noted in section 1.2.2.2.3, above, most courts would allow searches of computers, pagers, or other electronic storage devices "incident to arrest" without probable cause or a warrant, but that doctrine has been severely weakened by the 2009 *Gant* case. Now courts are divided as to whether police would need to get a 4.Amend. search warrant, or whether some other doctrine would allow warrantless access to the contents of electronic devices. A federal appeals court is considering whether cellsite locations stored, for instance, in smartphones deserve privacy protection, or whether they are "business records" that belong to the phone companies.405

Some courts have required a search warrant to search a confiscated cellphone or I-phone, even if the information could have been obtained by court order from the service provider.406 One federal court, however, determined that police may record numbers called on a pager when it is seized in the "on" position, because the suspect, in making the call to the pager, assumed the risk that his message would be received by whomever happened to be in possession of the pager at the time.407

1.8 Collecting Information from the Human Body for Purposes of Present and Future Identifications

1.8.1 Collection of Fingerprints and Other External Aspects of the Human Body

The USSC has ruled that citizens have no reasonable expectation of privacy in their exterior appearances, and therefore no right not to be photographed or placed in line-ups or other identification procedures during criminal investigations.408 Similarly, a person has no reasonable expectation of privacy in their fingerprints and can be compelled to submit fingerprints if the person has been lawfully detained.409 If a photo or fingerprints were taken after an unlawful detention, they may be subject to exclusion from trial as "fruit of the poisonous tree."410

Once one's photograph or fingerprints have been lawfully taken, however, then they may be compared with other photos or fingerprints, by human observation, or electronically.

1.8.2 Collection of Evidence Relating to the Interior of the Body

1.8.2.1 Extraction of Blood

The USSC recently decided that police need a search warrant to extract blood from a drunk driving suspect and may not rely on "exigent circumstances" based in the fact that the the body will naturally metabolize the alcohol in the bloodstream and lead to a loss of evidence.411

1.8.2.2 Collection of Material for the Purpose of DNA Analysis or Addition to DNA Data Bases

The 2000 DNA Analysis Backlog Elimination Act412 requires a person who "is or has been" convicted of a qualifying felony, to provide a DNA sample for the FBI's Federal Combined DNA Index System (CODIS) database. All states have similar laws and will forward information collected to the FBI to be entered into the CODIS system.413

---

402 United States v. Torres, 751 F.2d 875 (7th Cir. 1984)
403 United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992). For other similar decisions, see: United States v. Falls, 34 F.3d 674 (8th Cir. l994); United States v. Mesa-Rincon, 9ll F.2d l433 (l0th Cir. l990); United States v. Cuevas-Sanchez, 82l F.2d 248 (5th Cir. l987); United States v. Biasucci, 786 F.2d 504 (2d Cir.) (l986) and
State v. Page , 911 P.2d 513 (Alaska 1996).
404 United States v. Williams, 124 F.3d 411 (3d Cir. 1997).
405 Sengupta (NYT, 26 Nov 2012), commenting on cases in Rhode Island and Ohio requiring warrants, and in California and Washington State, not requiring them for text messages.
406 State v. Boyd, 992 A.2d 1071 (Conn. 2010).
407 United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990).
408 United States v. Wade, 388 U.S. 218 (1967).
409 Hayes v. Florida, 470 US 8ll (l985).
410 Davis vs. Mississippi, 394 US 72l (l969); United States v. Oscar-Torres, 507 F.3d 224 (4th Cir. 2007).
411 Missouri v. McNeely, 133 S.Ct. 1552 (2013).

Courts are divided, however, as to whether the collection of the samples is justified as an administrative "special need,"414 or just as an exercise of reasonableness clause balancing, due to the minimal nature of the seizure required to collect the sample.415

All States now require persons convicted of any felony to submit a biological sample and 28 states also require persons arrested of certain serious felonies to submit biological samples. The USSC recently upheld the taking of a bucal (cheek) swab from a person arrested on an assault charge as not violating the 4.Amend. It held that the bucal swab technique was less intrusive than drawing blood, and was "reasonable" in light of the administrative purpose of identifying perpetrators of past and future crimes. In so doing it rejected the "special need" analysis. The court equated the taking of DNA with that of fingerprints.416 Some states courts have invalidated statutes requiring the taking of DNA samples from all arrestees.417

As of 2006, 38 or more states required biological samples from some misdemeanants. The federal DNA-collection statute now authorizes the government to extract biological samples from illegal immigrants as well. Some statutes also apply to those acquitted by reason of insanity and even juveniles.418 As of 2006, 31 US jurisdictions required DNA samples from some juvenile offenders,419 and many of these statutes have survived challenges in the courts.420

Most courts have also held that further analysis of DNA samples, or their comparison with other samples does not constitute a "search" within the meaning of the 4.Amend.421

1.8 Law Enforcement Task Forces Involved in the Implementation of ICT Within the Criminal Justice System

1.8.1 Internet Crime Complaint Center (IC3)

First set up as the "Internet Fraud Complaint Center" in Morgantown, W.Va., in 1999, and renamed IC3 in 2002, the IC3 is a clearing house for the investigation of internet crime. It is a combined project of the FBI and the National White Collar Crime Center, a non-profit contractor to the DOJ, the US Postal Inspection Service (USPIS) and other organizations.422

1.8.2 Cyber Initiative and Resource Fusion Unit (CIRFU)

CIRFU was reated by IC3 and is located in Pittsburgh, Pa.. Its task is to eliminate false leads and refine a case before it is referred to prosecutorial agencies. It gets support from Microsoft, ebay, Paypal, AOL, Business Software Alliance, Direct Marketing Association, Merchant Risk Council and the financial services industry. Investigators and analysts from these private organizations have joined CIRFU to identify internet crime trends and technologies and develop significant cases.423

1.8.3 U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT is the 24-hour operational arm of the DHS's National Cybersecurity and Communications Integration Center (NCCIC). US-CERT was founded by the Defense Advanced Research Projects Agency (DARPA) and gives advice and serves as a repository of information related to computer crimes. While it carries out no investigation, it does coordinate with federal agencies, industry, the research community, and state and local governments to enhance the cybersecurity of the US.424

1.8.4 Infragard

InfraGard is an FBI program that began in 1996. In March of 2003 it became a part of the DHS. It is a partnership between the FBI and private individuals, academic institutions, state and local law enforcement agencies, and other participants dedicated to

---

412 42 U.S.C. § 14135 (2000)
413 State v. O'Hagen, 914 A.2d 267 (N.J. 2007).
414 United States v. Kimler, 335 F.3d 1132 (10th Cir. 2003); Nicholas v. Goord, 430 F.3d 652 (2d Cir. 2005); United States v. Hook, 471 F.3d 766 (7th Cir. 2007); State v. O'Hagen, 914 A.2d 267 (N.J. 2007); State v. Martinez, 78 P.3d 769 (Kan. 2003).
415 United States v. Sczubelek, 402 F.3d 175 (3rd Cir. 2005); Landry v. Attorney General, 709 N.E.2d 1085 (Mass. 1999); State v. Raines, 857 A.2d 19 (Md. 2004); Padgett v. Donald, 401 F.3d 1273 (11th Cir. 2005);
416 Maryland v. King, 133 S.Ct. 1958 (2013).
417 People v. Buza, 129 Cal.Rptr. 3d 753, 755 (Cal. App. 2011), cited in Kimel (2013, 940).
418 The New Jersey law applies to both. State v. O'Hagen, 914 A.2d 267 (N.J. 2007).
419 Kimel (2013, 939-40).
420 In re D.L.C., 124 S.W.3d 354 (Tex. App. 2003)(as to sex offenders); A.A. v. Attorney General of New Jersey, 914 A.2d 260 (N.J. 2007); In re Lakisha M., 882 N.E.2d 570 (Ill. 2008); Petitioner F. et al v. Brown, 306 S.W.3d 80 (Ky. 2010).
421 Boroian v. Mueller, 616 F.3d 60, 67 (1st Cir. 2010); State v. Hauge, 79 P.3d 131, 141-42 (Haw. 2003); People v. King, 663 N.Y.S.2d 610, 614 (App. Div. 1997), cited in Kimel (2013, 944). But for a spirited argument that such comparison should implicate the 4.Amend., see Kimel (2013, 943-70).
422 Larkin (2006, 40), https://www.ic3.gov
423 Larkin (2006, 40-41),
424 http://www.us-cert.gov/about-us/

sharing information and intelligence to prevent hostile acts against the US. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C. Before 9-11, its focus was cyber infrastructure protection, but since 2001 it now focuses on physical threats to critical infrastructures as well. The goal of InfraGard is to promote ongoing dialogue and timely communication between its members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.425

1.9 Databases Used in Law Enforcement and for Purposes of Data Mining

1.9.1 Public Databases

1.9.1.1 National Crime Information Center (NCIC)

NCIC, created in 1967, helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. It also assists law enforcement officers in performing their official duties more safely and provides them with information necessary to aid in protecting the general public. By the end of the fiscal year of 2011, when it averaged 7.9 million transactions per day, it contained 11.7 million active records. These records are collected in "files" dedicated to 21 different types of crimes.426

1.9.1.2 Integrated Automated Fingerprint ID System (IAFIS)

IAFIS, created in 1999, is a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year to help local, state, and federal law enforcement solve crime. It provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses. IAFIS includes not only fingerprints, but corresponding criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and aliases. The system also includes civil fingerprints, mostly of individuals who have served or are serving in the US military or have been or are employed by the federal government. The fingerprints and criminal history information are submitted voluntarily by state, local, and federal law enforcement agencies.

IAFIS is the largest biometric database in the world, housing the fingerprints and criminal histories for more than 70 million subjects in the criminal master file, including 73,000 known and suspected terrorists, along with more than 34 million civil prints. The average response time for an electronic criminal fingerprint submission is about 27 minutes. IAFIS processed more than 61 million ten-print submissions during Fiscal Year 2010.427

1.9.1.3 Uniform Crime Reporting (UCR)

The UCR Program, conceived in 1929 by the International Association of Chiefs of Police, is the original source for seeking reliable uniform crime statistics in the US. In 1930, the FBI was tasked with collecting, publishing, and archiving those statistics. UCR publishes reports, including "Crime in the United States," based on data received from over 18,000 local, state and federal law enforcement agencies voluntarily participating in the program.428

1.9.1.4 National Incident Based Reporting System (NIBRS)

The NIBRS, operational since 1998, is an incident-based reporting system in which agencies collect data on each single crime occurrence within 22 offense categories. NIBRS data come from local, state, and federal automated records' systems. The NIBRS can furnish information on nearly every major criminal justice issue facing law enforcement today, including terrorism, white collar crime, weapons offenses, missing children where criminality is involved, drug/narcotics offenses, drug involvement in all offenses, hate crimes, spousal abuse, abuse of the elderly, child abuse, domestic violence, juvenile crime/gangs, parental abduction, organized crime, pornography/child pornography, driving under the influence, and alcohol-related offenses.

The NIBRS has much more detail in its reporting system than does UCR because it collects information about more types of offenses and distinguishing between attempted and completed offenses. The NIBRS also collects information about crimes committed using a computer.429

425 https://www.infragard.org
426 http://www.fbi.gov/about-us/cjis/ncic
427 http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis
428 http://www.fbi.gov/about-us/cjis/ucr
429 http://www2.fbi.gov/ucr/faqs.htm

1.9.1.5 National Instant Criminal Background Check System (NICS)

The NICS, in existence since 1998, and located in Clarksburg, W. Va., is used to instantly determine whether a prospective buyer is eligible to buy firearms or explosives. Before ringing up the sale, cashiers call in a check to the FBI or to other designated agencies to ensure that each customer does not have a criminal record or isn't otherwise ineligible to make a purchase. More than 100 million such checks have been made in the last decade, leading to more than 700,000 denials. It provides service to 30 states and the District of Columbia.430

1.9.1.6 Law Enforcement National Data Exchage (NDEx)

The NDEx uses criminal justice data from local, state, tribal, and federal agencies across the nation to quickly "connect the dots" between data that may seem unrelated. It is a repository of criminal justice records, available in a secure online environment, managed by the FBI's Criminal Justice Information Services (CJIS) Division.

NDEx brings together data such as incident and case reports, arrest reports, computer-aided dispatch calls, traffic citations, narratives, photos, supplements, booking and incarceration data, and parole/probation information. It also automatically correlates and resolves data from open and closed reports to detect relationships between people, vehicles/property, locations, and/or crime characteristics. It also supports multi-jurisdictional task forces—enhancing national information sharing, links between regional and state systems, and virtual regional information sharing. No fees are charged and results are returned in a matter of seconds, based on the user's Internet connection.

The system can be used to conduct nationwide searches across jurisdictions, gathering information from various aspects of the criminal justice life cycle via a single access point, to conduct searches keyed to names,, phone numbers, tattoos, associates, cars, boats, modus operandi, etc. It may also be used to coordinate task forces, identify crime trends and use geovisualization and mapping features, identify "hotspots" of criminal activity and assess threats.431

1.9.1.7 CODIS and State and Local Analogues

The 2000 DNA Analysis Backlog Elimination Act (see section 1.8.2.2., above), requires a person who "is or has been" convicted of a qualifying felony, to provide a DNA sample for the FBI's CODIS database. All states have similar laws and will forward information collected to the FBI to be entered into the CODIS system.

Law enforcement agencies first send samples, usually of blood or saliva, voluntarily given by citizens, or taken from prisoners or other sources. to a state forensic laboratory, where state employees construct a genetic profile from the sample. Once created, the genetic profile is uploaded into CODIS. The uploaded information includes the profile itself, a specimen identifier, and identification of the laboratory and technician who generated the profile. As of September 2012, the national CODIS database contained more than 11,628,300 profiles, 11,176,400 of which were derived from voluntary donors and from categories of convicts, arrestees, and others whose DNA profiling is authorized or mandated by statute. When police conduct a CODIS search, they compare a profile generated from a crime-scene sample against each of the 11,176,400 profiles that constitute the national Offender Index.432

Law enforcement agencies have used these databases not only to solve countless "cold" cases,433 but also, since 1989, to exonerate at least 306 innocent persons.434

Local law enforcement agencies across the country have also begun assembling their own DNA databases, and amassing DNA samples sometimes from donors without their knowledge. These local databases operate under their own rules, providing the police much more leeway than state and federal regulations. Local police sometimes collect samples from far more than those convicted of or arrested for serious offenses, such as from innocent victims of crimes whose DNA was taken to "eliminate them as suspects" (say in the burglary of their own home), but who do not necessarily realize their DNA will be saved for future searches.

New York City has amassed a database with the profiles of 11,000 crime suspects. In Orange County, California, the district attorney's office has 90,000 profiles, many obtained from low-level defendants who give DNA as part of a plea bargain or in return for having the charges against them dropped. In Central Florida, several law enforcement agencies have pooled their DNA databases. A Baltimore database contains DNA from more than 3,000 homicide victims. As local authorities devise their own

430 http://www.fbi.gov/about-us/cjis/nics
431 http://www.fbi.gov/about-us/cjis/n-dex
432 Kimel (2013, 937-39).
433 As of January 16, 2009, there have been at least 79,000 "cold hits," that is, identifications of persons who were not earlier suspects in the particular unsolved cases. Kimel (2013, 940-41).
434 Robertson (NYT, 4 May 2013).

policies, they are increasingly taking DNA from people on the mere suspicion of a crime, long before any arrest, and holding on to it regardless of the outcome. Police somtimes ask for the samples, or sometimes collect them surreptitiously, say, from discarded trash. Alaska is alone in prohibiting local DNA databases.435

1.9.1.8 Terrorist Identities Datamart Environment (TIDE)

The TIDE contains about 700,000 names. It is the main repository from which other government watch lists are drawn, including the FBI's Terrorist Screening Database and the Transportation Security Administration's "no fly" list. Although Tamerlan Tsarnaev, was put on this list after notifications from the Russian government, the CIA did not consider him a threat and was caught by surprise when he planned the Boston marathon bombings in April of 2013.436

1.9.2 Private Databases Useful for Criminal Investigations

1.9.2.1 SWIFT

SWIFT is the Society for Worldwide Interbank Financial Telecommunication, a member-owned cooperative through which the financial world conducts its business operations with speed, certainty and confidence. More than 10,000 banking organisations, securities institutions and corporate customers in 212 countries exchange millions of standardized financial messages through SWIFT every day. The US takes advantage of this service.

1.9.2.2 Private Databases Designed for Commercial Use

In the US, commercial data brokers, such as Acxiom, Docusearch, DoubleClick, ChoicePoint, Oracle and Lexis-Nexis, track Internet and consumer spending habits of citizens and create extensive data profiles of American consumers. They then sell this data to companies who can target possible customers.437 The data includes basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal records, bank account balances and activity, stock purchases, and credit card activity. The government routinely makes use of these services. Even in the years before 9/11, ChoicePoint and similar services ran between 14,000 and 40,000 searches per month for the United States Marshals Service alone.438

Representatives of Oracle have stated that their database "is used to keep track of basically everything," and a representative of Google stated that the company's mission "is to organize all the information in the world."439

1.10 Programs for Accessing, Mining and Evaluating Data

1.10.1 Police Access to Databases While on Patrol

Traditionally, police would access databases on their office computers or, if out on patrol, on laptop computers carried in their police cars. These are sometimes not reliable, as it will often take time to connect with the Internet, so information about a developing situation may come to late.

The New York City Police Department and other departments around the country now are using dedicated Android smartphones which marshall a huge amount of information from collected databases. For instance, one can type in the address of a building and immediately have access to the names of every resident who has an outstanding arrest warrant or arrest record, each apartment which has had a prior domestic incident report, or is the target of a protection order. It shows who are registered gun owners and generates the photographs of every parolee in the building. . The phones enable officers on foot patrol, to look up a person's criminal history and verify their identification by quickly gaining access to computerized arrest files, police photographs, and state Department of Motor Vehicles databases. The phones can determine whether a person has been a passenger in a motor vehicle accident, a victim of a crime, or even where a suspect usually carries his illegal drugs.440

1.10.2 Government Data Mining Programs

The most norotious US data mining operation no longer exists. "Total Information Awareness" (TIA) caused a scandal when the public found out it was run by John Poindexter, one of the main conspirators in the Iran-Contra scandal in the 1980s and it was defunded in 2003.441 Shortly after the demise of TIA, the government spent at least $40 million developing another data

435 Goldstein (NYT, 13 Jun 2013).
436 Schmitt, Schmidt (NYT, 15 Apr 2013).
437 Casey (2008, 1006); Slobogin (2008, 320).
438 Slobogin (2008, 320).
439 Slobogin (2008, 327)
440 Ruderman (2013, A17).
441 Slobogin (2008, 317)

mining program called ADVISE (for Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement). More recently, it has become entranced with the concept of "fusion centers," a mixture of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information regarding individuals by mining data about banking and finance, real estate, education, retail sales, social services, transportation, postal and shipping, and hospitality and lodging transactions. As of September 2006, there were thirty-eight State and local government Information Fusion Centers, supported by $380 million in federal funding.442

The Defense Department sponsors the largest number of data mining operations. One such program is called Verity K2 Enterprise, which mines data from the intelligence community and internet searches in an effort to identify foreign terrorists or US citizens connected to foreign intelligence activities. Another is known as Pathfinder, which provides the ability to rapidly analyze and compare government and private sector databases. There is also TALON (Threat and Local Observation Notice), a program which has collected information on thousands of American citizens involved in protesting the war in Iraq and other government policies, and made the data accessible to 28 government organizations and over 3,500 government officials. A fourth Defense Department program has accumulated files on hundreds of Americans suspected of being spies, which contain information from their banks, credit card companies, and other financial institutions..443

The DOJ, through the FBI, has been collecting telephone logs, banking records, and other personal information regarding thousands of Americans not only in connection with counterterrorism efforts. The most prominent effort in this regard is the FBI's System-to-Assess-Risk (STAR) program, which makes use of the Foreign Terrorist Tracking Task Force "Data Mart," consisting of a wide array of sources, to acquire more information about suspected terrorists and other "persons of interest." but also in furtherance of ordinary law enforcement. 444

Finally, the Snowden revelations in June 2013 unveiled the program "XKeyscore" which the US government not only itself uses, but also provided to the German Federal Constitutional Protection Service which is used when the NSA or other services intercept all communications data from a particular cable. It filters out useful information in clear text and registers metadata as well as content data if it conforms to specific buzz words. It can also trail the originators of the e-mails in real time by tracking the location of messages sent, etc.445

1.10.3 Private Data Mining Programs

An example of a private data mining program is Accurint, owned by LexisNexis, which boasts to be able to, in mere seconds, "search tens of billions of data records on individuals and businesses," armed with no more than a name, address, phone number, or social security number. All of this was for a time made accessible to state law enforcement officials with the establishment of MATRIX (Multi-state Anti-terrorism Information Exchange), a consortium funded in part by the federal government that allowed state police to use Accurint for investigative purposes. 446

1.11 The Problem of Secret Interception of Data With No Notification Provisions and Its Shared Use by National Security and Criminal Enforcement Organs

1.11.1 The Right to Discover Whether One Was a Target of Secret Surveillance

As has been noted above, the government need not inform a person that he or she has been the subject of FISA surveillance, nor whether the government has installed pen/trap devices, or gathered stored communications metadata or electronic communications by subpoena or NSL directed to service providers.

In the wake of the revelation of the secret NSA interceptions during the administration of George W. Bush, several lawsuits were filed by NGOs on behalf of persons attempting to ascertain whether they had their confidential communications intercepted during that long-term operation. An Islamic charity sued President Bush and other executive branch entities, alleging that it was subjected to warrantless electronic surveillance under the NSA program, but the government claimed that the "state secrets" privilege prevented it from revealing the information for the purposes of the lawsuit.447

The American Civil Liberties Union (ACLU) sued the government on behalf of a group of lawyers and journalists alleging that the program violated FISA and that they had likely had their conversations intercepted thereunder, and another group of citizens sued AT& T on account of its collaboration with the allegedly illegal NSA program. In both cases, the government moved to

442 Slobogin (2008, 318).
443 Slobogin (2008, 319)
444 Slobogin (2008, 319-20)
445 Pfister et al (2013, 18).
446 Slobogin (2008, 320-21).
447 Al-Haramain Islamic Foundation Inc. v. Bush, 507 F.3d 1190 (9th Cir. 2007)

dismiss the suits, either on the ground that the plaintiffs lacked standing, i.e., could not prove their conversations were intercepted, or because "state secrets" would have to be revealed in defending the suit. In both cases, the plaintiffs were ultimately denied relief based in the allegation of "state secrets."448

The US chapter of Amnesty International challenged the NSA wiretap program on behalf of certain lawyers, human rights, labor, legal and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad. The complaint alleged that some of the persons with whom the plaintiffs communicated could be people that the government believes are associated with terrorist organizations and that the provision of the 2008 amendments of FISA, 50 U.S.C. §1881a, which allow such surveillance, would prevent them from engaging in their livelihood through the use of international correspondence by telephone or e-mail. The USSC denied the plantiffs standing, claiming they could present no clear evidence that their conversations had been intercepted, or that future threatened injury was "certainly impending" and thus no "case or controversy" existed which the court could entertain.449

The government's lawyer in *Clapper*, in his arguments, alleged that the only way a person could have "standing" to challenge secret NSA wiretaps, and to find out if her communications were intercepted in the first place, would be if she were charged in court and the government filed a notice of intent to use the intercepted communications in its case.

Nevertheless, in subsequent prosecutions, federal prosecutors have refused to make the promised disclosures, even after charges have been filed, thus undercutting the assurances the government lawyer had made to the USSC in *Clapper*.450 *

1.11.2 "Hand-Off" Procedures to Avoid Notification Requirements of Title III or other Laws

The wiretap "hand-off" procedure was used by investigators in Los Angeles beginning in the 1980s. It involves an initial issuance of a wiretap order by a judge. Once the wiretap yields evidence of criminal conduct, the investigating agents would then transmit the information to another unit without expressly stating that the information was discovered through a wiretap. The receiving unit then conducts further investigation. Evidence gathered during that second investigation would yield independent probable cause to arrest the targets. The defendant would be prosecuted without ever knowing that he was subjected to the wiretap surveillance. 451

"Hand off" procedures were also apparently the main tool used to develop the material gathered in the secret NSA surveillance programs. This arguably illegally gathered information was secretly fed back into the established legal system of telecommunications surveillance. It has been estimated that from 10 to 20% of FISA warrants annually are based on information gathered in the secret NSA domestic surveillance program.452

The secret NSA program has led, in the words of one commentator, to a "secret parallel system of telecommunications surveillance," where information collected in it is fed back into the official system in a fashion that leaves no traces. The system is "built on secret presidential authorizations, secret DOJ legal opinions; nonbinding presidential promises; an executive that refuses to provide Congress and the public with necessary information; and, most recently, acquiescent congressional legislation enacted in ignorance of the true dimensions of NSA activities."453

1.11.3 The Problem of Removing the "Wall" Between Traditional Law Enforcement and National Security Information Gathering

Since involvement of the Army and CIA in domestic surveillance of anti-Vietnam-War and Black Power activists in the 1960s and 1970s, there was a concerted effort to separate traditional law enforcement from intelligence gathering. This so-called "wall" between the two arms of government meant that only FISA would be used for intelligence wiretaps and Title III for conventional organized crime investigations. Although the President had authority prior to the enactment of FISA to conduct national security wiretaps, federal courts would exclude evidence gained from such wiretaps when it turned out that the investigation had become, primarily, a conventional criminal enforcement operation.454

448 ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007); Hepting v. AT&T, 439 F.Supp.2d 974 (N.D.Cal. 2006). See discussion in Casey (2008, 979-80, 1020-25).
449 Clapper v. Amnesty International, U.S.A.,133 S.Ct. 1138, 1148-49 (2013).
450 Liptak (NYT,16 Jul 2013).
451 Whitaker v. Garcetti, 291 F.Supp.2d 1132 (C.D.Cal. 2003).
452 Schwartz (2008, 307).
453 Schwartz (2008, 309).
454 United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

Even before 9-11, however, evidence legally gathered through a FISA wiretap could be used in a criminal prosecution against a US person.455 After 9-11, however, the standard for a FISA wiretap was lowered to require only that a "significant purpose" of the wiretap was aimed at foreign intelligence, instead of the "primary purpose" language that existed in the original version of FISA. The Patriot Act intentionally aimed at removing the so-called "wall." This made it more easy for FISA wiretaps to be simultaneously used for foreign intelligence as well as for conventional criminal investigation. And, with the lower threshold, as long as the wiretap can be justified under FISA, the evidence may be used in a conventional criminal prosecution as well.456 The FISA Appeals Court has also ruled conclusively that there is no harm in "sharing" of material between law enforcement and intelligence operatives and that no such "wall" ever really existed.457

1.11.4 The Search for a New Paradigm

It is becoming clear to more scholars, judges, and the public in the US, that the traditional 4.Amend. approach to privacy protection is obsolete in the digital age. Even before the revleations of Edward Snowden in June, 2013, Justice Sotomayor, in *United States v. Jones* indicates that it is time for a change. She wrote:

> " [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers (...). I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.458

For the new generation of users of social media, such as Facebook, Twitter, Linked-In, etc., electronic communications of feelings and ideas can be seen as a surrogate for conversations which might earlier have taken place in a protected place like a home or a telephone conversation. The fact that one must enlist a service provider to facilitate these exchanges, according to this opinion, is not a sufficient reason for denying the protection that the 4.Amend. gives to homes, and telephone conversations.459

The USSC has gradually extended the realm of privacy, first in the home, with decisions preventing use of a thermal imager (*Kyllo*) or a canine sniff (*Florida v. Jardines*), and even in automobiles, with the limitation of searches incident to arrest under *Gant*. But the decision in *Jones* and the strong concurring opinions of Justices Sotomayor and Alito, along with State court and lower federal court decisions limiting long-term surveillance in public places by GPS or cellphone location, seem to indicate a trend in the courts of recognizing the new necessities of protection in this era of massive use of ICT and the switch in the understanding of the population on what should be kept from government eyes.

This new approach to the 4.Amend., reflected in the concurring opinions in *Jones,* focusing on the totality of the actions of law enforcement in its surveillance of a suspect, and not on whether each sequential step taken by law enforcement comports or not with USSC interpretations of the 4.Amend, i.e., was, or was not a "search" according to the high court's jurisprudence, has been labeled a "mosaic theory" of the 4.Amend.460 This approach appears to denigrate the traditional "inside-outside" demarcations which characterized the court's jurisprudence: i.e., all in the house, in private is protected, all in public, revealed to a third person, "envelope" information, is not.461

455 United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Nicholson, 955 F.Supp. 588 (E.D.Va. 1997); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988)
456 United States v. Ning Wen, 471 F.3d 777 (7th Cir. 2006).
457 In re: Sealed Case No's 02-001, 02-002, 310 F.3d 717 (USFIS App. 2002).
458 United States v. Jones, 132 S.Ct 945, 957 (2012).
459 Ghoshray (2012, 82-85); McAllister (2012, 499-500).
460 In general, see Kerr (2012).
461 Supporting the "inside-outside" approach and rejecting the "Mosaic" approach, see Kerr (2012, 346-53).

The outrage at the new revelations, by Edward Snowden, of the massive NSA data mining and surveillance aimed at US citizens and foreign citizens and governments, is also indicative of the fact that the USSC's interpretation of the 4.Amend. is falling behind the times. Sociological studies have shown, indeed, that the majority doctrines applied by the USSC in relation to using pen registers, GPS tracking devices, or cellphone site location do not correspond to the expectations of privacy held by a significant majority of society.462

Some critics suggest a rejection of the "reasonable expectation of privacy" test in favor of a test based on expectations of "security" from government intrusion, thus returning to the language of the 4.Amend. which says that the people should be "secure in their persons, houses, papers and effects."463

In the area of data mining, Christopher Slobogin suggests that we should reject the one-size-fits-all approach of USSC case law that treats all information given to a third party as lacking 4.Amend. protection. He feels simple subpoenas should suffice for obtaining corporate and most public records, but probable cause and a warrant should be required to obtain records containing the most personal information, such as bank records, telephone records and ISP logs. A court order, based on reasonable suspicion, on the other hand, would suffice when the government sought to obtain records that are quasi-private, such as power consumption, or school records.464

Slobogin differentiates between target-driven searches, such as those mentioned above, and "event driven" cases where public or quasi-public information is matched in response to an investigation of a crime, in order to identify possible suspects. Since these types of searches only involve matching one or two bits of information (whether a person lived in a certain city during a certain period or bought a particular type of shoe). Here one's record is is merely one of hundreds or thousands, and will be discarded or at least ignored if it does not prove of interest to investigators. For this type of data mining, no judicial order would be needed.465

The uproar about the Snowden revelations nearly led to the US House of Representative imposing restrictions on the powers of the NSA to intercept *en masse* communications metadata,466 and there is evidence that the public is losing confidence in the spy agencies, CIA and NSA, and the government in general due to the phone and internet surveillance, the use of Drones, and the earlier scandals around the use of torture.467 Hopefully this means that changes may be on the way.

2. USE OF ICT TO PRESERVE EVIDENCE

2.1 The Recording of Confessions

2.1.1 States Which Require the Recording of Confessions

There is no general requirement of US evidence law, or of 5.Amend. law which requires that confessions be audio-, or video-recorded. Critics of the famous decision of *Miranda v. Arizona*,468decision have always maintained that the recording of confessions would be sufficient to mitigate the coercive nature of custodial police interrogation so as not to require the famous warnings as to the right to silence and right to counsel which that opinion introduced into American police procedure.

As of 1990, however, about one-third of all police and sheriffs' departments in the US which served populations of 50,000 or more were videotaping at least some interrogations.469 Despite the growing use of recording, only a handful of states have required, either by statute, or by high court rule-making, that custodial police interrogations be audio-, or video-recorded. 470 Missouri passed a law in 2009 requiring recording of confessions if "feasible" but provides no sanctions if a confession is not recorded, thus eliminating any teeth from the provision.471

462 McAllister (2012, 512-29); Slobogin (2008, 333-36).
463 Casey (2008, 1028).
464 Slobogin (2008, 337).
465 Slobogin (2008, 338).
466 The vote was 205 to 217. Weisman (NYT, 25 Jul 2013).
467 Shane (NYT, 26 Jul 2013).
468 Miranda v. Arizona, 384 U.S. 436 (1966).
469 Dressler, Thomas (1999,598).
470 Stephan v. State, 711 P.2d 1156 (Alaska 1985); State v. Scales, 518 N.W.2d 587 (Minn. 1994); State v. Barnett, 789 A.2d 629 (N.H. 2001); Commonwealth v. Diaz, 661 N.E.2d 1326 (Mass. 1996). Minnesota and New Hampshire have explicitly not extended the recording requirement to out-of custody interrogations: State v. Conger, 652 N.W.2d 704 (Minn. 2002); State v. Velez, 842 A.2d 97 (N.H. 2004).
471 § 590.700, RSMo (2011).

A few States require exclusion of a confession if it was not electronically recorded,472 while others entitle the defendant, upon request, to a jury instruction concerning the need to evaluate his statement or confession with "particular caution" if it was not recorded.473

2.1.2 The Admissibility of Secretly Recorded Confesssions by Undercover Agents

Although it is clearly legal to record a police interrogation in all US jurisdictions, and if the confession complies with the *Miranda* decision and the subsequent cases interpreting its scope, and is deemed to be voluntary, such recording will clearly be admissible in court as evidence.

When, however, a jailhouse informant or undercover police officer secretly induces a suspect to confess, or to give otherwise incriminating admissions, the USSC has issued a number of opinions which basically differentiate between the treatment of charged and uncharged suspect-accuseds.

First of all, as long as police agents do not "interrogate" a defendant, and only place a recording device in a prison cell or interview room to record what the defendant says to, for instance, a private citizen or another prisoner, the recording is clearly admissible.474 Thus incriminating statements made by co-arrestees and recorded surreptitiously in the back of a police car are admissible, first, due to lack of a reasonable expectation of privacy and therefore absence of need for a Title III warrant,475 but also because there has been no police "interrogation."476

The USSC has also ruled that the *Miranda* rules do not apply when jailhouse informants secretly interrogate uncharged prisoners, because the prisoner is unaware that he is being interrogated and therefore, according to the Court, is not subject to the coercive atmosphere of police custody.477 On the other hand, if a defendant has been charged and is represented by counsel, then any surreptitious interrogation by an informant is seen to violate the 6.Amend. right to counsel, which only applies after one is charged, even if the defendant is out of custody.478 If the defendant is in-custody, a jailhouse plant may record incriminating statements made by a defendant as long as the informant is only listening, or at least not actively inducing incriminating remarks.479 Informants may also surreptitiously interrogate (and record) charged defendants if they interrogate them crimes with which they have not yet been charged.480 As long as these complex rules are followed, a recorded confession will be admissible.

3. ICT AND THE ADMISSIBILITY OF EVIDENCE

3.1 Introduction

As was thoroughly discussed in the above chapters, ICT information in the form of wiretaps or external "envelope" activity involving communications in the form of pen registers, trap and trace devices or websites visited is admissible as long as neither the 4.Amend. has been violated, nor the more rigid requirements of Title III or FISA.

Otherwise, ICT information is admissible in criminal cases as long as it otherwise comports with the rules of evidence, i.e., it must be relevant and material to the case,481 must be reliable, and must abide by the rules governing hearsay and the right of the defendant to confront and cross-examine witnesses guaranteed by the 6.Amend. The general rule is that all witnesses must testify orally in open court before the trier of fact, whether jury or judge.482 For any taperecording, or business record showing trap and trace or pen register information to be admissible, the officers conducting the wiretap or bugging operation must testify as to how they carried out the surveillance, to the chain of custody of the tapes, etc. The custodian of business records must also always testify as to whether information as to, for instance, telephone calls, was kept in the "ordinary course of business" and lay a foundation for the entry of the evidence into the trial record.

472 Davidson v. State, 25 S.W.3d 183 (Tex. Crim. App. 2000)(even if the interrogation was made by a federal officer in a State without such a rule). In re Jerrell C.J., 699 N.W.2d 110 (Wis. 2005)(limited to confessions of juvenile defendants).
473 Commonwealth v. DiGiambattista, 813 N.E.2d 516 (Mass. 2004). But see United States v. Bruce, 550 F.3d 668 (7th Cir. 2008), where defendant was not allowed such an instruction in a federal case based on a confession taken in violation of a state recording rule.
474 Arizona v. Mauro, 481 U.S. 520 (1987).
475 See section 1.3.1.2, above.
476 State v. Edrozo, 578 N.W.2d 719 (Minn.1998).
477 Illinois v. Perkins, 496 U.S. 292 (1990).
478 Massiah v. United States, 377 U.S. 201 (1964).
479 United States v. Henry, 477 U.S. 264 (1980); Kuhlmann v. Wilson, 477 U.S. 436 (1986).
480 Maine v. Moulton, 474 U.S. 159 (1985).
481 Federal Rules of Evidence (FRE) 401, 402.
482 F.R.Crim. P. 26.

3.2 Rules Governing the Integrity of ICT Information

Other than the specific exclusionary rules provided in Title III and FISA, there are also detailed rules dealing with preserving the tapes of conversations recorded pursuant to the two wiretap acts, giving the defendant a chance to hear the tapes, and provisions for when the recordings can be destroyed.

The general rules of evidence give the defendant and the prosecution the power to challenge the admissibility of evidence, by claiming it was tampered with, is not what it claims to be, etc. The party proposing the admission of the evidence must show that there has been proper chain of custody of the evidence and defend any challenges that the evidence was tampered with, etc.

When dealing with recordings, generally the original recording must be admitted into evidence.[483] Duplicates or copies are admissible however, unless "a general question is raised as to the authenticity of the original."[484] Other evidence of the contents of a recording are admissible if the original is no longer available, or if the recording is not relevant to a controlling issue in the case.[485]

3.3 Rules Governing Discovery and Disclosure of ICT Information

3.3.1 Introduction

As has already been discussed, the person affected by a Title III wiretap must eventually be informed of the fact that the operation took place. Under FISA, in relation to wiretaps, sneak and peek searches, capturing of metadata, and national security letters, however, investigators can delay revelation of the investigative measure if there is a "danger to the investigation." Otherwise, the general rules of discovery govern whether or not and when the prosecution must reveal ICT evidence to the defense, if a prosecution has been commenced.

3.3.2 Discovery of Statements of the Defendant or Witnesses Contained in ICT Information

More than one half of the States have a comprehensive discovery statute regulating which evidence must be turned over by the prosecution to the defense. Federal discovery rules are laid out in F.R.Crim. P. 16, and about a dozen states follow the federal model.

Although written or recorded statements by the defendant must be turned over to the defense in all jurisdictions, there are limitations when such a statement is part of a conversation recorded by an informant, or through wiretapping or bugging. Fed. R. Crim. P. l6(a)(1)(A) limits disclosure to oral or recorded statements of the defendant that were made "in response to interrogation" to a person "then known to the defendant to be a government agent" and thus would not include statements in an intercepted telephone conversation or made to undercover informants.[486] Most States, however, require the prosecutor to turn over statements of the defendant of any kind if the prosecutor intends to introduce them at trial.

On the other hand, the federal prosecutor need not identify the witnesses he or she intends to call at trial, nor turn over their statements prior to their actually having testified in court.[487] Around 20 States, however, require recorded statements of witnesses to be turned over to the defense.

The prosecution is required by due process to turn over to the defendant any exculpatory evidence, including evidence which impeaches the credibility of prosecution witnesses, or evidence which might mitigate punishment.[488] This would certainly be the case of a wiretap that tended to show the innocence of the defendant. However, there are limits to which the prosecutor must scour tapes of telephone conversations to look for exculpating evidence.[489]

It is routine, however, for the defense to subpoena or request discovery of the telephone conversations or dispatches of police officers at or around the time of the defendant's alleged commission of a crime, in order to determine a witness's earliest description of the suspect, or to otherwise impeach the testimony of the arresting officer.[490]

---

483 FRE 1002.
484 FRE 1003.
485 FRE 1004.
486 F.R.Crim. P. 16(a)(1)(A), 16(a)(1)(B)(ii).
487 F.R.Crim. P. 16(a)(2); 18 U.S.C. § 3500. Around one-third of the States have a similar rule.
488 Brady v. Maryland, 373 U.S. 83 (1963)
489 In United States v. Merlino, 349 F.3d 144 (3d Cir. 2003) the court said that the fact that a few conversations of informants had exculpatory character did not mean that the police had to review all conversations between the informants.
490 For instance, see State v. Ortiz, 215 P.3d 811 (N.M. App. 2009), in which the court allowed discovery of all communications to and from the arresting officer on his cell phone during a six minute period for reasons of possible impeachment.

3.3.3 The Classified Information Procedures Act of 1980 (CIPA)

If, as has been done in the case of secret wiretaps and searches under FISA related to anti-terrorism and national security, the government claims that disclosure of the wiretaps or other information secretly gathered will either constitute the revelation of state secrets, or other classified information, then the court must proceed under the procedure set out in CIPA. 491

Since 9-11, the federal government has maintained, that all evidence gathered during terrorist investigations is secret, or "classified," the revelation of which would prejudice national security and impede the war against terrorism.492

Traditionally, the more urgent the state's interest was in protecting the secrecy of classified information, the greater was the opportunity for the defense to induce or even extort a dismissal of the charges by moving to discover the delicate information. CIPA was promulgated in 1980 in an attempt to balance the right of the defense to discover evidence in the hands of the prosecution against the needs of the state to protect information which was crucial to national security. CIPA attempted to minimize the defense threat to reveal secret evidence during the trial, a practice called "graymail." According to CIPA, "classified inforsmation" consists in any information or material determined by US government to "require protection against unauthorized revelation for reasons of national security."493 A typical "graymail" case is where a former employee of the C.I.A., charged with criminal wrongdoing, threatens to reveal, or to use in his defense, evidence the government considers to be classified.

If the defendant seeks discovery of information which is "classified" or contains state secrets, the judge may authorize the prosecutor to "eliminate classified information in the documents which are turned over to the defense" or to substitute it with a summary of the information in lieu of the secret documents themselves, or to offer a declaration, admitting the relevant facts which the classified information would have a tendency to prove."494 The prosecutor can request that the hearing be heard *in camera* by alleging that a public hearing would result in the revelation of classified information.495 If a summary or substitution finding of fact is deemed by the trial judge to not satisfactorily protect the rights of the defendant to present a defense, the court may order full disclosure

3.4 The Admissibility of ICT Information in the Form of Statements of the Defendant or Other Participants in the Proceedings in Light of the Hearsay Rule and the Defendant's Right to Confront Witnesses

3.4.1 Admissibility of the Statements of Defendants Contained in ICT Material

"Hearsay" is defined as a statement, whether oral or written or even an assertion by gestures, which was made outside of the trial, but is introduced at trial to prove "the truth of the matter asserted."496 The general rule is that hearsay is inadmissible evidence, except where exceptions have been provided by statute or court decision (including doctrine of the Common Law, unless repudiated by court or statute).497 Thus, in general, a statement made by a suspect-defendant, whether as a result of interrogation, or in a legally intercepted communication, is "hearsay."

The Common Law, however, has traditionally considered that statements of parties to a legal proceeding, whether civil or criminal, are admissible, either as an "exception" to the hearsay rule which forbids the admission of hearsay, or as "non-hearsay."498 The rule of admissibility extends to any statements, even those not recorded and proffered in court by police officers or jailhouse informants. As a result, huge amounts of potentially false or distorted "statements" by defendants have been admitted with no safeguards for their veracity, and these have led to many wrongful convictions, a significant number of them in capital cases.499

491Classified Information Protection Act, Pub.L. 96-456 (94 Stat. 2025), Oct. 15 1980, codified at 18 U.S.C. app. 3 et seq.
492 The government was even allowed to keep secret the names and locations of the many Muslims detained after 9-11, claiming revelation would hamper national security. Center for National Security Studies v. U.S. Department of Justice, 331 F.3d 918 (D.C.Cir. 2003).
493 18 U.S.C. app.3 § 1(a).
494 18 U.S.C. app.3 § 4
495 18 U.S.C. app.3 § 6(a).
496 FRE 801(a,c).
497 FRE 802.
498 FRE 801(d)(2) treats such statements as "non-hearsay."
499 In more than 15 % of the convictions of the innocent overturned after DNA analysis, crucial testimony was given by undercover informants. The Innocence Project, http://www.innocenceproject.org/understand/Snitches-Informants.php At least 142 death sentences have been passed against innocent persons since 1976. Death Penalty Information Center. Facts About the Death Penalty, Updated June 7, 2013, http://www.deathpenaltyinfo.org/documents/FactSheet.pdf

There is also a long-standing hearsay exception for "statements against penal interest" which applies if the declarant is unavailable to testify in court. This would thus apply to a defendant who has exercised his or her right to remain silent as protected by the 5.Amend.500

3.4.2 Introduction of Prior Statements to Impeach a Testifying Witness

Once a witness is called to testify, is sworn, and gives direct testimony, all jurisdictions allow the opposing party to present to the witness prior statements, whether formal statements to investigating officials or statements from legally intercepted conversations, to attempt to undermine the testimony given in court.501 In some jurisdictions, these "hearsay statements," can be admitted to prove the truth of the matter stated. In the federal courts, prior testimony or depositions made under oath are admissible when used to confront a testifying witness, who then may be cross-examined as to their content.502

3.4.3 Introduction of Statements of Witnesses: Exceptions to the Hearsay Rule

Some types of statements were traditionally admissible as exceptions to the hearsay rule, because of their supposed inherent veracity, whether or not the declarant was unavailable to testify at trial. Any of the following hearsay exceptions could be contained in recordings of intercepted conversations: (1) statements of "present sense impression" which describe or explain an event or condition while the declarant was perceiving the event or condition; (2) "excited utterances," made in relation to a "startling event or condition" while the declarant was under the stress of excitement caused by the event or condition; (3) statements of "existing mental, emotional, or physical condition;" and (4) statements for the purpose of medical treatment.503

Another well-accepted exception to the hearsay rule related to so-called "dying declarations" made by a person "under belief of impending death," the reliability of which is presumed because no one would lie and risk going to Hell on his or her deathbed. Such statements were traditionally only admissible if the person had, indeed, died and was unavailable to testify.504

3.4.4 The Right to Confront and Cross-Examine Witnesses: A Sixth Amendment Exclusionary Rule Based on Whether the Statement is "Testimonial"

In the landmark case of *Crawford v. Washington*,505 the USSC reverted back to a strict rule of exclusion for statements given by non-testifying and non-available witnesses where the person giving the statement had never been subject to cross-examination by the defendant. The court stated that "the principal evil at which the Confrontation Clause was directed was the civil-law mode of criminal procedure, and particularly its use of *ex parte* examinations as evidence against the accused."506 In the 1980s and 1990s, the USSC allowed prior statements taken down by the police to be admitted if they either "fell under a firmly-rooted hearsay exception" or had otherwise evinced "particularized guarantees of trustworthiness."507 In *Crawford*, however, the USSC overruled that precedent, and fashioned a strict exclusionary rule for "testimonial hearsay" which clearly included statements taken by police in the preparation of a criminal case, affidavits or prior testimony the defendant never was able to subject to cross-examination.508 The *Crawford* court opined that most of the hearsay exceptions, such as for business records, do not apply to "testimonial" utterances, but it clearly stated that, with the exception of dying declarations, there would be no other blanket exceptions recognized for testimonial hearsay.509 If the declarant was not available to testify and had not been subject to cross-examination as to the subject matter at a prior proceeding, the statement would be *prima facie* inadmissible.510

Of course, many statements or assertions are made through ICT in telephone calls to the police, conversations where police or their informants are listening in to conversations without needing a Title III or FISA warrant, or even in confidential conversations intercepted with a valid judicial order. When citizens call the police to report a crime that is ongoing or has just happened, the statement may be an "excited utterance" or a statement of "present sense impression" but it may also be given with knowledge that it can and will be used in a criminal investigation or prosecution.

The USSC has ruled in the context of such emergency 911 calls, that hearsay statements made during questioning by law enforcement officials are "testimonial" for purposes of the Confrontation Clause, when the "primary purpose" of the questioning

500 FRE 804(b)(3).
501 F.R.Crim. P. 26.2(a); FRE 613.
502 FRE 801(d)(1).
503 FRE 803(1-4).
504 FRE 804(b)(2).
505 541 U.S. 36 (2004).
506 541 U.S. at 50.
507 Ohio v. Roberts, 448 U.S. 56, 66 (1980), overruled by *Crawford*.
508 541 U.S. at 41-42.
509 541 U.S. at 55.
510 448 U.S. at 58.

was to establish facts for a later prosecution, but not when the caller's primary purpose is to aid police in relation to an ongoing emergency or crime. Thus, the taped phone call of a woman who calls police while being battered by her husband could be used in a prosecution of her husband, if she is unavailable to testify in court due to marital privilege or other reasons.511 If the statement to police, even though "excited" takes place after the emergency is over, it might be treated as "testimonial" and therefore be inadmissible,512 but just using the past tense in one's descriptions may not be sufficient to qualify a statement as "testimonial."513 A victim's description of an assault to civilians or family immediately thereafter 514 or even to police dispatchers515 is also not necessarily "testimonial."

The USSC recently declared that police questioning of a wounded man, who later died, as to the identity of the man who shot him, qualified as "non-testimonial" under the test in *Davis*.516 This does not, however, mean that "dying declarations" will always pass the 6.Amend. test.

A doctrine had developed, whereby the statement of a witness, not subject to cross-examination by the defendant, could be used in court, if the defendant caused her failure to appear in court. The USSC, however, rejected this "forfeiture-by-wrongdoing" exception, if the prosecutor could not show that the defendant, at the time he engaged in the wrongful acts that rendered a declarant unavailable, was acting with an intent to prevent the declarant from testifying.517 Without this narrowing, any statement made in response to a police question by an assault victim could be used in court if the victim were to die of his or her wounds. Before *Giles*, most courts had treated true dying declarations as exceptions to the *Crawford* rule,518 and this continues to be the practice afterwards.519

Courts have also dealt with cases involving confidential conversations using ICT following the *Crawford* decision. A Florida court held that statements of a non-testifying co-defendant made in a telephone conversation between him and the defendant were "testimonial" and therefore inadmissible, because the co-defendant, who let police listen in to and record the conversation, was working as a police informant and was questioning in this capacity.520 However, other courts have admitted secretly recorded under-cover conversations between suspects and confidential informants as "non-testimonial"521 or developed sophisticated tests to distinguish when they are, or are not.522 In the last analysis, it appears, however, that normal conversations by suspects amongst themselves who do not realize there conversations are being intercepted, will not qualify as "testimonial" and therefore will be admissible at trial.

A policeman's recorded simultaneous description of criminal activity he is observing, although in the strictest sense qualifying as admissible under the hearsay-exception of "present sense impression" is "testimonial" under the *Crawford* test and inadmissible in some courts,523 but others, relying on the hearsay-exception, have held them to be "non-testimonial."524

The right to confrontation guaranteed by the 6.Amend. also guarantees defendants the right to cross-examine experts who prepare scientific reports or analyses.525 The prosecution must call the person who actually prepared a report and not another expert for purposes of explaining the contents of a report.526 However, the USSC recently split its opinion on the issue of whether a testifying expert could refer to a conclusion of a non-testifying expert posed as a hypothetical, with four judges finding

511 Davis v. Washington, 547 US 813, 822 (2006)
512 State v. Kirby, 908 A.2d 506 (Conn. 2006).
513 State v. Ohlson, 168 P.3d 1273 (Wash. 2007).
514 State v. Slater, 939 A.2d 1105 (Conn. 2008); Clarke v. United States, 943 A.2d 555 (D.C.App. 2008).
515 People v. Johnson, 189 Cal.App.4th 1216 (Cal. App. 2010).
516 Michigan v. Bryant, 131 S.Ct. 1143 (2011).
517 Giles v. California, 554 U.S.353 (2008)
518 See, for instance, People v. Durio, 794 N.Y.S.2d 863 (N.Y. Sup. 2005); Harkins v. State, 143 P.3d 706 (Nev. 2006); State v. Lewis, 235 S.W.3d 136 (Tenn. 2007).
519 State v. Jones, 197 P.3d 815 (Kan. 2008); State v. Beauchamp, 796 N.W.2d 780 (Wis. 2011).
520 State v. Hernandez, 875 So.2d 1271 (Fla. App. 2004).
521 State v. Johnson, 771 N.W.2d 360 (S.D. 2009)(recording of conversation during undercover drug purchase).
522 State v. Smith, 960 A.2d 993 (Conn. 2008).
523 Shennett v. State, 937 So.2d 287 (Fla. App. 2006).
524 United States v. Solorio, 669 F.3d 943 (9th Cir. 2012).
525 Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009).
526 Bullcoming v. New Mexico, 131 S.Ct. 2705 (2011).

no violation of the Confrontation Clause, because the questionable opinion of the non-testifying expert was not "hearsay" because it was not admitted for the truth of the matter stated.527

Federal evidence law recognizes an "omnibus" or residual hearsay exception for statements that have "equivalent circumstantial guarantees of trustworthiness," like the traditional hearsay exceptions, which are more probative than other evidence that could go to prove the same disputed fact, and where the "interests of justice" require admission of such statement.528 This exception was a basis for admission of much hitherto inadmissible hearsay before the *Crawford* decision, but now that exception would seemingly only apply in cases of non-testimonial hearsay or in civil cases.

3.5 The Admissibility of ICT Information Not in the Form of Statements of Witnesses or the Defendant

One major traditional exception to the hearsay rule was for "business records," or "records of regularly conducted activity" which are "made at or near the time" by a person with knowledge of the substance of the record, if the record was kept "in the course of a regularly conducted business activity."529 Another was for "public records or reports setting forth the activities of the office or agency" or "matters observed pursuant to a duty imposed by law" (with the exception of police reports).530

Regarding the "business records" exception to the hearsay rule, which apparently survived *Crawford*, it occasionally comes into play in relation to the use of ICT evidence. For instance, one court decided recently that a bank robber's confrontation rights were not violated when prosecutors introduced, as business records, the "tracking reports" generated by a GPS device that was hidden in the bag of stolen cash a teller gave him.531 Another court, however, found a violation when the trial judge admitted into evidence reports compiled by an internet service provider implicating the defendant in the collection and trading of child pornography without giving him a chance to cross-examine the employees who drafted those reports.532

4. THE USE OF ICT IN THE COURTROOM

4.1 The Use of Technology to Transmit Witness Testimony from Afar

4.1.1 The Use of Closed-Circuit Television to Transmit Live Testimony into Court

The USSC has allowed the use of one-way closed-circuit television to present the live testimony of a young childwitness in a child sex abuse trial, justifying this exception to the "face to face" confrontation requirement533 if there is a strong public policy reason for making the exception. It found this policy applicable in such cases because a young child might be so intimidated by the presence of the defendant in such a trial, that the child might be unable to testify truthfully, or at all. In that case, the prosecutor and defense counsel examined the child in another room and the examination was transmitted into the courtroom, where the judge, defendant and jury were located. The USSC also noted that at the time of the decision in 1990, 37 States allowed use of the videotaped testimony of allegedly abused children, 24 States allowed the use of one-way closed circuit television, and another eight allowed the use of two-way closed circuit television, where the child in the courtroom could see the witness testifying off-site.534

One federal court held that the strict *Craig* test, requiring a strong public policy reason was limited to the use of one-way closed-circuit television, and that two-way closed circuit television would be applicable without such a strong public policy reason, as long as the requirements for a deposition under F.R.Crim. P. 15 (see below) have been complied with.535

Although the USSC has not revisited this issue since its landmark decision in *Crawford*, most courts who have dealt with the issue have ruled that the stricter *Crawford*-rules have not affected the decision in *Craig* and that the used of closed-circuit television is still admissible when young children are testifying in such cases.536

New York has a statute that authorizes vulnerable children to testify by video in sex cases, but the State's highest court said this did not bar judges from applying the statute to other cases, such as the trial of a home health aide who was charged with

527 Williams v. Illinois, 132 S.Ct. 2221 (2012) . The vigorous four-judge dissent has been followed by at least one court. State v. Navarette, 294 P.3d 435 (N.M. 2013).
528 FRE 807.
529 FRE 803 (6).
530 FRE 803(7).
531 United States v. Brooks, 715 F.3d 1069 (8th Cir. 2013).
532 United States v. Cameron, 699 F.3d 621 (1st Cir. 2012).
533 Pronounced by the USSC in Coy v. Iowa, 487 U.S. 1012 (1988) (rejecting placement of screen between testifying witness and defendant).
534 Maryland v. Craig, 497 U.S. 836 (1990).
535 United States v. Gigante, 166 F.3d 75 (2d Cir. 1999). See also State v. Sewell 595 N.W.2d 207 (Minn.App. 1999), in which the court allowed the testimony of an injured victim by "interactive television."
536 State v. Henriod, 131 P.3d 232 (Utah 2006).

assaulting an 83-year-old man who, by the time of trial, was too frail to travel to court. The victim was allowed to testify by two-way video from a California courtroom where he could see the judge, jury, counsel, and defendant, and they could see him, including his facial expressions.537 The USSC refused to grant certiorari in this case and let the decision of the New York court stand.538

However, if the prosecution cannot convince the court of exception or compelling reasons, the videotaped deposition of out-of-state or out-of-country witnesses will not be allowed simply because of the convenience of not paying for their trip to the US or to the State in which the trial is being held. For instance, it was reversible error in a prosecution for fraud and conspiracy, to allow two Australian witnesses to testify via two-way video, when there was no important public policy other than the convenience of not paying for their trip to the US.539 A State court also barred the prosecution from presenting the testimony of a witness by telephone in the absence of a compelling reason.540

Generally, courts addressing the issue of the use of two-way closed circuit television or video conferencing after *Craig*, *Crawford*, and *Yates* have fallen into three camps. First, some courts have followed *Yates*, and applied the *Craig* test.541 Secondly, some courts have determined that the two-way technology protects the 6.Amend right to confrontation and that no specific findings were necessary. Finally, some courts refuse to permit two-way technology now, but leave open the possibility that video-conferencing will be common in the future.542

4.1.2 The Use of ICT in the Creation of Pre-trial Depositions

One method of avoiding the strictures of the *Crawford* decision is to arrange for a pre-trial deposition of a witness who may be in danger of not appearing at trial due to illness, threats, or residence in a foreign country. The film and audio recording of such a deposition would then be admissible at trial, as long as the defendant had a right to confront and cross-examine the witness as required by the 6.Amend.

F.R.Crim.P. 15 regulates depositions in the federal courts. A court may grant a motion for a pretrial deposition upon a finding of "exceptional circumstances and in the interest of justice."543 If the defendant is in custody, jail officials must make sure he/she is brought to the place of the deposition.544

If the deposition is conducted using two-way video, as is allowed in the case of child complainants in sexual assault cases in some jurisdictions, with the defendant in a different location, the defendant must be guaranteed instantaneous communication with his lawyer or the 6.Amend. is violated.545

When the government conducts a deposition in a foreign land with a view toward introducing it in a US criminal trial, the 6.Amend. requires, at a minimum, that the government undertake diligent efforts to facilitate the defendant's presence at the deposition and the witness's presence at trial.

A court was held to have "diligently" undertaken to secure the defendant's appearance at a deposition in the United Kingdom, where it directed the US government to transport the defendant's attorney to the deposition and install two telephone lines – one to allow the defendant to monitor the deposition from prison and another to allow him to consult privately with counsel. 546

In a case involving an alleged Al-Qaeda affiliate charged with a number of terrorist acts in the US, including conspiracy to assassinate President George W. Bush, the validity of a handwritten confession given by the defendant in Saudi Arabian custody was at issue. Because it was impossible to bring two Saudi officials, whom the defendant accused of torturing him, to the US, the trial court ordered two defense attorneys to attend their depositions in Saudi Arabia. A live, two-way video link was used to

537 People v. Wrotten, 923 N.E.2d 1099 (N.Y. 2009).
538 Wrotten v. New York, 130 S.Ct. 2520 (2010), cited in Brooks (2012, 186).
539 United States v. Yates, 438 F.3d 1307, 1316 (11th Cir. 2006). But for a case allowing two robbery victims to testify by video link from Argentina against the person who allegedly robbed them during a visit to the U.S., see Harrell v. Butterworth, 251 F.3d 926, 928-31 (11th Cir. 2001).
540 State v. Moore, 56 P.3d 1099 (Ariz.App. 2002). Note, however, a case where a federal court allowed a victim to just confirm her social security number through a telephone connection. United States v. Schuler, 458 F.3d 1148 (10th Cir. 2006).
541 Horn v. Quarterman, 508 F.3d 306, 320 (5th Cir. 2007)(permitting terminally ill patient to testify); United States v. Bordeaux, 400 F.3d 548, 554-55 (8th Cir. 2005).
542 Brooks (2012, 202-03), citing People v. Buie, 775 N.W.2d 817, 824 (Mich. 2009).
543 F.R.Crim.P.15(a)(1).
544 F.R.Crim.P.15(c)(1).
545 United States v. Miguel, 111 F.3d 666 (9th Cir. 1997)
543 United States v. McKeeve, 131 F.3d 1, 8-9 (1st Cir. 1997).

transmit the proceedings to a courtroom in Virginia, where the defendant and his lawyer could see and hear the testimony contemporaneously and the witnesses could see and hear the defendant as they testified. The court found that national security against terrorist acts was a sufficiently compelling public policy." 547

Courts have also allowed videotapes of a deposition conduct abroad through tele-conferencing to be used at trial.548

4.2 The Use of ICT to Bring the Defendant into the Courtroom

4.2.1 Arraignment and other Pretrial Proceedings

Courts have permitted the use of closed circuit television to facilitate a defendant's "appearance" in court at arraignment and other pretrial proceedings.549 For instance, video-conferencing has been used at a motion to suppress evidence in federal courts.550

Where the hearing involves the entry of a guilty plea, however, the defendant has a right to be physically present, though this right may be waived and the appearance can be made through closed circuit television or video-conferencing.551

4.2.2 Presence at Sentencing

Defendants have an absolute right to be present during trial and sentencing, and such right is violated if video conferencing is used to connect him to court from his jail cell.552

4.3 Use of Digital and Virtual Technology at Trial Other Than to Present Witness Testimony

4.3.1 Digitalization of the Presentation of Documentary Evidence at Trial

As of 2003, over 350 federal district courts had installed large computer monitors to display electronic evidence to the jury. Over 32 federal courtrooms had been certified as high technology courtrooms, which means they have the ability to transmit electronic evidence anywhere in the world and receive video messages via two-way video conferencing. Two-way video technology had, by 2003, been authorized for courtroom use in over 29 States. These numbers have certianly grown, as courts acknowledge the advantages modern technology. A number of jurisdictions have even begun discussing the possibility of "virtual trials" where all components of the trial, including evidence, opening statements, closing statements, parties, the jury, and the judge will be in different locations and transmitted electronically.553 There are, of course, limitations to holding a "virtual trial" in a criminal case as we have discussed above.

Before trial, litigators commonly utilize electronic filing programs, electronic docketing, online case management, and e-mail communication with the court.554

4.3.2 Use of Digital and Virtual Technology During Closing Arguments

During trial prosecutors and defense counsel often take advantage of what high-tech courtrooms have to offer, presenting electronic displays and PowerPoint presentations to the jury. Early studies have shown that juries appreciate the benefits of electronic evidence and "want evidence to be presented visually to the greatest degree possible."555

4.4 ICT and Maintaing the Impartiality of the Trial Jury

4.4.1 ICT and Jury Selection

The wide-spread use of social media, such as Facebook, Twitter, Linked-In, etc. have presented difficulties in selecting juries in criminal cases. When there is a notorious crime, typically a sensational murder case, news of the arrests, the early investigative measures, etc. go "viral" on the internet, leading to case-specific creation of web-sites and social media pages.

As a result, defense lawyers, when selecting juries must play close attention to on-line communities that may be generated by a headline-grabbing case they may be involved in. Jury consultants have also begun studying the attitude of members of jury

547 United States v. Abu Ali, 528 F.3d 210, 238-43 (4th Cir. 2008).
548 US v. Nippon Paper Industries Co. 17 F.Supp.2d 38 (D.Mass. 1998).
549 People v. Lindsey, 772 N.E.2d 1268 (Ill. 2002).
550 United States v. Burke, 345 F.3d 416 (6th Cir. 2003).
551 State v. Soto, 817 N.W.2d 848 (Wis. 2012).
552 United States v. Navarro, 169 F.3d 228 (5th Cir. 1999); United States v. Torres-Palma, 290 F.3d 1244 (10th Cir. 2002); United States v. Lawrence, 248 F.3d 300 (4th Cir. 2001); United States v. Williams, 641 F.3d 758 (6th Cir. 2011).
553 Brooks (2012, 212).
554 Brooks (2012, 212).
555 Brooks (2012, 212-13)

pools by monitoring on-line discussions of the issues in a particular case. Information from web discussions might be one factor in inducing the judge to grant a motion for a change of venue.556

Lawyers and prosecutors may also legally run an on-line analysis of the prospective jurors by running their names through public records databases or common search engines, or even use a tool called "Social Mention" which allows the searching of blogs, networks, videos, will send daily e-mail alerts regarding the prospective juror.557 Judges, of course, could resort to the use of anonymous juries to counteract this invasion of the privacy rights of the jurors.558

4.4.2 Sequestration of the Jury and Access to ICT

4.4.2.1 Juror Use of ICT to Augment or Challenge the Evidence

The jury in a criminal case should base its decision only on the evidence introduced at trial. However, with the use of smartphones or I-pads, jurors can download information from the internet and use this in deliberations to convince other jurors of a point under discussion.

Courts have occasionally had to deal with this problem. In one case, in which the defendant was charged with the shaking death of her 4-month-old stepgrandchild, the prosecution presented evidence that the defendant was taking daily dosages of the antidepressant Paxil for stress and depression. When the judge denied the jury permission to consult pharmacological references, one juror downloaded a description of the drug from the Internet and shared it with the other jurors the next day. This constituted reversible error, because the web description could have affected the outcome of the case.559 In another case, the conviction of a Somali Bantu immigrant for sexual assault was reversed because one juror researched Somali mores and beliefs on the internet and shared the results with fellow jurors.560

A federal appellate court has held that when a juror consults extrajudicial information, such as an online database, prosecutors can save a conviction only if they can overcome a presumption that the juror's misconduct was prejudicial to the accused's right to a fair trial.561

Judges can clearly prevent such conduct during actual courtoom deliberations by confiscating all portable devices for accessing the internet while the jury deliberates. However to prevent accessing the internet during evening recesses, the court would have to sequestrate the jury for the entirety of the trial, which would make jury trial even more costly than it now is.

4.4.2.2 Juror Use of ICT to Communicate With Others During Deliberation

During the taking of the evidence, jurors are daily instructed that they must not discuss the case either with other members of the jury, or anyone else, such as close friends or family, until they have reached a verdict. Clearly, the court can prevent any contact by confiscating all mobile phones, I-phones, smartphones and the like during the trial, though complete sequestration is the only method to definitely prevent any such discussions.

Convictions have been reversed when jurors have used mobile phones or cell phones or other devices to engage in impermissible discussions of the case. For instance, a capital murder conviction was reversed when one juror continued to post messages to his Twitter account about the trial, even after the trial judge admonished him to stop.562

When a judge finds out a juror has been using a social media program, such as Facebook, courts have held that the judge must hold a post-conviction hearing on potential juror bias. this was done in a case where two jurors may have used their Facebook accounts to "friend" a victim's mother.563 In another case, the court compelled a juror, who had commented about the evidence on his Facebook page during trial, to authorize Facebook to release for *in camera* review all the items he posted during the trial.564

556 Brown (2013, 820-21).
557 Brown (2013, 827-28)
558 Normally anonymous juries are only allowed for high-publicity organized crime cases where there is a potential threat to the security of jurors. See, for instance, United States v. Tutino, 883 F.2d 1125 (2d Cir. 1989). However a judge kept the names of jurors secret during jury selection in a high-publicity child-murder case, that of Casey Anthony, and then revealed their names after the trial started. Brown (2013, 831).
559 People v. Wadle, 97 P.3d 932 (Colo. 2004).
560 State v. Abdi, 45 A.3d 29 (Vt. 2012).
561 United States v. Lawson, 677 F.3d 629 (4th Cir. 2012).
562 Dimas-Martinez v. State, 385 S.W.3d 238 (Ark. 2011)
563 Sluss v. Commonwealth, 381 S.W.3d 215 (Ky. 2012).
564 Juror Number One v. Superior Court of Sacramento County, 142 Cal.Rptr.3d 151 (Cal.App. 2012).

5. ICT POST-TRIAL

6.1 Proving Innocence Through the Use of DNA Data Banks

6.1.1 The Problem in the US of the Conviction of the Innocent

Nationally, 306 convicted felons have been exonerated between 1989 and May of 2013 based on evidence collected in the nation's DNA data banks.565 142 prisoners on death row have been exonerated of capital crimes since 1976, many of them due to DNA analyses that proved their innocence.566

6.1.2 Access to DNA Data Banks for the Purpose of Proving Innocence

Although almost every state has a law permitting some post-conviction DNA testing, only nine--Colorado, Georgia, Illinois, Maryland, Mississippi, New York, North Carolina, Ohio and Texas--have laws granting defendants access CODIS.567 In some states, a motion for post-conviction testing may not be denied just because the defendant confessed to the crime at the foundation of his conviction.568

Despite the compelling social interest in clearing the names of the innocent that have been sentenced for crimes they did not commit, the USSC has ruled that the due process guarantees of the US Constitution do not include the right to retest bodily fluids gathered during a criminal investigation to prove one's innocence, even if one has offered to pay for the testing.569

At least one state has also decided that a capital prisoner cannot compel the state to test the DNA of a third party to see if it matches the DNA of a hair found on the murder victim, so as to exclude him as the perpetrator of the murder.570

565 Robertson (NYT, 4 May 2013).
566 Death Penalty Information Center, see above.
567 Bronner (NYT, 4 Jan 2013). On CODIS, see section 1.8.2.2, above.
568 Commonwealth v. Wright, 14 A.3d 798 (Pa. 2011).
569 District Attorney's Office for the Third Judicial District v. Osborne, 557 U.S. 52 (2009).
570 Isom v. State, 372 S.W.3d 809 (Ark. 2010).