2017

The Use of Information and Communications Technology in Criminal Procedure in the USA

Stephen C. Thaman

SAINT LOUIS UNIVERSITY SCHOOL OF LAW
Legal Studies Research Paper Series

No. 2017-22

Cybercrime, Organized Crime, and Societal Responses: International Approaches

Chapter Six: The Use of Information and Communications Technology in Criminal Procedure in the USA

Stephen C. Thaman
Emeritus
Saint Louis University - School of Law

Springer International Publishing Switzerland, 2017

Emilio C. Viano
Editor

Cybercrime, Organized Crime, and Societal Responses

International Approaches

Springer

Editor
Emilio C. Viano
International Society of Criminology
Washington, DC, USA

ISBN 978-3-319-44499-4 ISBN 978-3-319-44501-4 (eBook)
DOI 10.1007/978-3-319-44501-4

Library of Congress Control Number: 2016948731

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To the memory of my parents, Giuseppe and Teresa Viano, who taught me, with their example, the value of commitment, work, and perseverance and who have encouraged and supported me in my studies and career with their generosity and sacrifices.

Chapter 6
The Use of Information and Communications Technology in Criminal Procedure in the USA

Stephen C. Thaman

Introduction

Law enforcement organs in the USA 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 private communications; and (3) the surveillance of transactions in which people engage (Slobogin 2005).

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 solve 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" (Slobogin 2008).

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 USA. After a discussion of this foundational case law, we 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 USA. We 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 compare the rules for normal criminal cases, with the special regimes applying to

S.C. Thaman (✉)
Saint Louis University School of Law, 100 N. Tucker Avenue,
St. Louis, MO 63101-1930, USA
e-mail: thamansc@slu.edu

E.C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses*,

investigations relating to national security and antiterrorism. We will also discuss the data bases which are key to government criminal investigations, and the private enterprises that cooperate, voluntarily or under threat of law, with the data mining and surveillance efforts.

Collecting Information as to Movements and Activities in Public Spaces

Use of Surveillance Cameras and Facial 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 (*State v. Holden* 1998), or in front of public establishments such as bars (*State v Augafa* 1999). Use of motion-activated video cameras in "open fields" is also permissible without judicial authorization (*United States v Vankesteren* 2009). Recording street-corner drug deals, either from a distance by using "bionic ears" and binoculars (*Stevenson v State* 1996), or by outfitting an informer's automobile with a video camera have not violated State privacy protections (*State v Clark* 1996). Using cameras in semipublic places like hospitals (*United States v Gonzalez* 2003), or open businesses (*Cowles v State* 2001) 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.

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

It was also recently revealed, that the NSA has been gathering "millions" of images per day of people from communications it secretly intercepts, of which around 55,000 per day are of sufficient quality to apply increasingly sophisticated facial recognition technology (Risen and Poitras 2014).

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 (Automatic Number Plate Recognition 2015). Oakland, California received $12 million in federal grants to use on antiterrorist surveillance at its large port, but it has instead used the money for massive surveillance related to ordinary law enforcement, "from gunshot-detection sensors in the barrios of East Oakland to license plate readers mounted on police cars patrolling the city's upscale hills" (Sengupta 2013b).

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 passenger.

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 (*United States v Boyce* 2003; *United States v Fernandez* 2010; *People v Harris* 2008). Other courts, however, allow prolongation for a reasonable time to consummate the warrant check (*State v Williams* 2003).

No individualized suspicion is needed to run the name of either a driver or a passenger through the national computer system (*State v Sloane* 2008).

Use of Tracking Devices

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 (*United States v Knotts* 1983).

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 (*United States v Karo* 1984). 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 (Goldstein 2015).

2. The Use of Global Positioning 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* (2012a, b) 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 4-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. (McAllister 2012, p. 493).

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 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 Governments 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 (*United States v Jones* 2012a, b).

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 (*United States v Jones* 2012a, b).

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 (*United States v Garcia* 2007; *State v Jackson* 2003; *People v Weaver* 2009; *United States v Maynard* 2010; *United States v Jones* 2012a, b), but others have followed their approach after the decision (*State v Zahn* 2012; *State v Brereton* 2013; *Commonwealth v Rousseau* 2013). Several states require a warrant before GPS devices may be used (see McAllister 2012, p. 506).

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 (Casey 2008, p. 1009). 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 (*United States v Forest* 2004; *Devega v State* 2010; *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government* 2010; *State v Subdiaz-Osorio* 2014).

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 Stored Communications Act (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 (18 USC §§ 2701–12; see Fox 2012, p. 771).

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 (*In re Application of the United States for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. & Cell Site Info* 2005). This decision was followed by 15 "pen register" decisions in other lower federal courts. In 11 of these cases, the courts have refused to issue the order and in four, they have allowed gath-

ering 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 (Fox 2012, p. 783), whereas the other required only "reasonable grounds" for the discovery of prospective CSLI, which involved monitoring future movements of the suspect (*In re Application of the United States for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. & Cell Site Info*2005, citing *In re Application of the U.S. for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices* 2008). 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" (McAllister 2012, pp. 518–520). A federal appeals court recently adopted this argument and held that historical CSLI held by service providers are "business records" and not protected by the 4.Amend. (*In re Application of United States for Historical Cell Site Data* 2013).

The trend appears to be in the direction of requiring a probable cause warrant to disclose cellsite location (Casey 2008, p. 1016; For cases requiring a warrant and probable cause, see *In re Application of the United States* 2011; *In re Application of the United States*, S D Tex 2010; *In re Application of the United States* E D N Y 2010, cited in (McAllister 2012, 520).

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 (Sengupta 2012).

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 (Risen and Lichtblau 2013).

In addition, NSA, working with its British counterpart, have expanded their surveillance in a program called "mobile surge," to include the many "leaky apps" used by smartphone and android phone users which spew out information, accessible by NSA, not only about the user's location, sex, and age, but which also make accessible address books, buddy lists, telephone logs and the geographic data embedded in photographs when someone sends a post to the mobile versions of Facebook, Flickr, LinkedIn, Twitter and other Internet services. A special target of the program

is also "Google maps" which reveals a large amount of information about the movements of those spied upon (Glanz et al. 2014). The NSA and the British have also been infiltrating the world of video games, because they think that potential terrorists use these games to communicate. The spy agencies have themselves created make-believe characters in the games, which they hope will be attractive to terrorists (Mazzetti and Elliot 2013).

The Use of Drones

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, Virginia, 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, Virginia passed a 2-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 (Sengupta 2013a).

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 3000 alleged terrorists in Afghanistan, Pakistan, Yemen, and Somalia, and in doing so, have caused considerable collateral casualties (Shane 2013a). The Drone strikes have also killed four Americans, including Anwar al-Awlaki (Savage and Baker 2013).

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" 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 (Worth et al. 2013). The revelations of Edward Snowden have also

shown that the NSA is also deeply involved in gathering information for use in target killings (Miller et al. 2013).

Uproar over this highly suspect use of Drones has led Congress to discuss whether a new secret court, like the Foreign Intelligence Surveillance Court (FISC), should be established to decide on which persons should be targeted for execution (Shane 2013b). 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 (Shane 2013c).

Collecting Information as to Activities in Homes and Other Private Spaces

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 indoor 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 details, because the entire area is held safe from prying government eyes" (*Kyllo v United States* 2001).

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 (*United States v Kattaria* 2007).

In March of 2013, the USSC avoided, however, deciding whether a "canine sniff" of a dwelling was a "search" by claiming that the officer and dog illegally

trespassed on the front doorstep of the house, thereby making the sniff the fruit of the illegal trespass (*Florida v Jardines* 2013). 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 (*United States v Thomas* 1985; *State v. Young* 1994). 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 (*State v Ortiz* 1999; *State v Davis* 2007; Some courts even require reasonable suspicion for the canine sniff of an automobile, *State v Wiegand* 2005; *State v Tackitt* 2003; *People v Devone* 2010).

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 (Adler 1996, p. 1098). After the decision in *Kyllo* 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," had proved useless against suspects clever enough to encrypt their files.

Magic lantern installs the 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 (Sullivan 2001).

Before *Kyllo* 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 a "magic lantern" key logger device on a defendant's personal computer and using the device to discover the passphrase to an encrypted file (*United States v Scarfo* 2001).

There are three main approaches to remote searches of computers through the use of "Trojan Horse" or "Magic Lantern"-type technologies. Twenty-two 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 (Brenner 2012, p. 54).

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 (*United States v Villegas* 1990; *United States v Villegas* 1999).

"Sneak and peek" warrants were codified with the passage of the US PATRIOT Act in October 2001, which amended the law (§ 213 US PATRIOT Act; 18 USC § 3103(a)), 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 (18 USC § 2705(a)(2)). Such "sneak and peek" searches are also allowed, upon warrant issued by the FISC, subject to similar conditions as required for FISA wiretaps (50 USC §§ 1822–24). 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" (50 USC § 1825(b)).

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

Warrants to Seize and Search Computers in the Home

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 on the computer's hard drive may be searched for and copied (*State v Ruck* 2013, computer legally seized in probation search, but warrant required to search hard drive). 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 computer so as to separate relevant files from unrelated files (*Guest v Leis* 2001).

1. Probable Cause that Illegal Files Will Be Found on a Computer

Law enforcement investigators will often note a specific internet account or internet protocol showing that a person accessed a child pornography website and 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 (*United States v Kennedy* 2000; *United States v Hambrick* 1999; *United States v Forrester* 2008, cited in Kerr 2010, pp. 1026–1027; *United States v Martin* 2005; *United States v Gourde* 2006; *United States v Wagers* 2006; *United States v Shields* 2006; *United States v Frechette* 2009). Other courts, however, require more evidence (Another panel of the Second Circuit strongly disagreed with the *Martin* decision but felt it had to upheld a similar case due to *stare decisis* (*United States v Coreas* 2005). 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 (*United States v McArthur* 2009).

2. 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 (*State v Rupnick* 2005). 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 (*United States v Upham* 1999).

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 (*United States v Bradley* 2011). 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 (*United States v Bridges* 2003).

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 (*Massachusetts v Sheppard* 1984). 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 (*United States v Kouzmine* 1996).

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 (*United States v Hill* 2006). The Nebraska Supreme Court also found a search warrant for a mobile phone to be overbroad for not specifying what conversations or data was to be seized (*State v Henderson* 2014). The Kentucky Supreme Court, however, recently held that a search warrant need not specify the component of the cell phone which was to be searched (*Hedgepath v Commonwealth* 2014).

3. 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 (Kimel 2013, p. 962).

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 (*Andreson v. Maryland* 1976). Some courts apply this broad approach to a search of a computer (*United States v Richards* 2011; *US v Giberson* 2008; *United States v Christie* 2013). 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" (*United States v Hill* 2006; *United States v Adjani* 2006).

A minority of courts, however, require special search protocols to limit the exploratory nature of searches of computerized material. In a similar vein, one federal judge has recently criticized DOJ officials for submitting patently overbroad warrants for searching suspects' e-mail accounts, whereas other courts will allow officers to look at each e-mail first to see if it fits within the scope of the warrant (Apuzzo 2014).

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 (see *United States v Carey* 1999). If the photo file has a tag that seems to indicate possible child pornography, then the "plain view" doctrine might apply (*Frasier v State* 2003). Some courts have approved

broad applications of the 4.Amend.'s plain-view doctrine to uphold sweeping searches of suspects' personal computers (*United States v Mann* 2010; *United States v Williams* 2010).

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 (*United States v Comprehensive Drug Testing, Inc* 2010).

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" (*People v Gall* 2011). Other 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 (*United States v Paxton* 2009).

4. 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 (*United States v Al-Marri* 2002; *United States v Lucas* 2011, consented to search of house or narcotics and "records" related to narcotics sale). 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 (*United States v Ziegler* 2007).

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 (*United States v Andrus* 2007). In another case, police relied on the apparent consent of defendant's girlfriend who had spent the night at defendant's abode and was allowed to use his computer and discovered child pornography (*State v Sobczak* 2013). A Texas court actually found that a man who gave a babysitter a tour of the master bedroom in which a computer was located, "consented" to the babysitter's use of the computer (*Baird v State* 2013).

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 pornography in image files (*People v Prinzing* 2009). Consent to search a premises for a person, for instances, could not be extended to searching a computer in the house (*United States v Turner* 1999). 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 (*United States v Reyes* 1996).

At least one court has refused to apply the rule of *Georgia v. Randolph* (2006), to a situation where one computer user refuses to let police search the computer in the presence of another user (*United States v King* 2010).

5. 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 (*Doe v United States* 1988).

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 (*Fisher v United States* 1976; *United States v Doe* 1984). 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 (*United States v Hubbell* 2000).

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 (*Fisher v United States* 1976; *United States v Doe* 1984).

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 (*United States v Kirschner* 2010; discussed in Bales 2012, p. 1302). 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 (*In re Grand Jury Subpoena Duces Tecum* 2012; cited in Bales 2012, pp. 1302–1303).

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 (Engel 2012, pp. 568–569). 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 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 (*United States v Fricosu* 2012; discussed in Engel 2012, pp. 563–566). The Massachusetts Supreme Judicial Court also, while recognizing that being compelled to provide encryption tools is "testimonial," held that the defendant's possession of the tools and ability to decrypt had already been revealed through his own boasting (*Commonwealth v Gelfgatt* 2014).

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 (Engel 2012, pp. 568–569).

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 (Schwartz 2008, p. 293). In addition, NSA has used "supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age," according to documents disclosed by Edward Snowden. The NSA hacked into computers to record messages before they were encrypted, and coerced some companies to turn over their master encryption keys. It also secretly introduced weaknesses into the encryption standards used around the world. The NSA spends more than $250 million a year in its Sigint Enabling Project which is designed to undermine commercial encrypting programs. This massive assault on encryption devices, code-named "Bull Run," has achieved what the Clinton Administration failed to do with its attempt to compel installation of a "clipper chip" in the 1990s (Perlroth et al. 2013).

Use of Informants to Electronically Surveil Activities in the Home

Since the string of decisions ending with *United States v. White* (1971), 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. The theory is that the suspect has "assumed the risk" of communicating with him or in his presence (see *Almada v State* 1999). Using a wired informer has even been allowed when the informer did not speak the language, nor understand the contents of the recorded conversation (*United States v Longoria* 1999).

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" (*United States v. White* 1971).

Several States have followed the dissents in *White* and required police to secure a judicial warrant before sending a wired informant into a dwelling (*People v Beavers* 1975; *State v Glass* 1978; *Commonwealth v Brion* 1995; *State v Bridges* 1997; *State v Geraw* 2002; *State v Mullens* 2007), or at least the approval of a high-level prosecutor (*State v Worthy* 1995, based on reasonable suspicion).

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 (*United States v Yonn* 1983; *United States v Myers* 1982; *United States v Lee* 2004). Other federal courts would, however, require judicial authorization under Title III (the wiretap statute) in such a situation (*United States v Padilla* 1975).

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. (*United States v Davis* 2003; *United States v Wahchumwah* 2012). If government authorities cannot gain consensual entrance into a home to use secret recording devices or video cameras, then they must obtain judicial authorization which follows the guidelines set out in Title III, the wiretap statute.

Video Surveillance in the Home

Although secret videotaping in a home or other private space is not covered in Title III, the US wiretap statute, nor considered to be an "interception" under that statute (*United States v Torres* 1984), 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 (*United States v Koyomejian* 1992; see also *United States v Falls* 1994; *United States v Mesa-Rincon* 1990; *United States v Cuevas-Sanchez* 1987; *United States v Biasucci* 1986; *States v Page* 1996). 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 (*United States v Williams* 1997).

Access to Electronically Stored Information in Private Possession in General

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

In 2014, the USSC tightened its rule on searches incident to arrest in holding that police could no longer treat a computer or smart phone as a mere "container" searchable without probable cause or a warrant after the arrest of its possessor. Barring exigent circumstances police must now get a search warrant to access the stored information on such a device (Riley v. California, 2014).

Some courts have required a search warrant to search a confiscated cellphone or iPhone, even if the information could have been obtained by court order from the service provider (*State v Boyd* 2010). 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 (*United States v Meriwether* 1990).

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

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" to obtain such information. 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.

Banking and Financial Transactions

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 (12 USC § 3410–22). 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 (*Miller* 1976). 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 allows the customer a period of time to object to the release of the records (*State v McAllister* 2004). Other States also give enhanced protection (*People v Nesbitt* 2010; *People v Mason* 1999, requiring "probable cause" for the issuance of a subpoena).

It recently became known that the CIA has secretly been gathering massive amounts of information about international money transfers without resorting to subpoenas or court orders. This practice has been supposedly authorized by the FISC, but the government has refused to make the decisions which allegedly did so public. The CIA claims the practice is authorized by the Patriot Act (Savage and Mazzetti 2013).

2. Cooperation Required by Financial Institutions

Banks are required by the Bank Secrecy Act of 1970 (BSA) (Pub L 91-508), 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 keeps them in computerized storage and makes them accessible to law enforcement (Thaman 2001). These provisions have been upheld by the USSC (*California Banker's Ass'n* 1974).

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 (*People v Stanley* 1999), in

pharmacy prescription records (*State v Russo* 2002), or in medical records from a public health clinic (*State v Mubita* 2008; *Commonwealth v Efaw* 2001).

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 (*In re Maxfield* 1997). 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 (*State v Jordan* 2007; *In re Pers Restraint of Nichols* 2001). Some courts also require a search warrant for prescription drug records (*Douglas v Dobbs* 2005; State v. Skinner).

Mail Covers

"Envelope information" is the metaphor used for communications metadata, 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. In its voracious appetite for data, the US government has instituted 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 USA, 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 15,000–20,000 per year. Officials need probable cause, and a warrant, of course to open a letter (Nixon 2013, 2014).

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

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

The government need not inform a person that he or she has been the subject of surveillance under the Foreign Intelligence Surveillance Act (FISA), 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. As a matter of fact, no lawyer has ever gotten discovery of the records which gave rise to a FISA search since the promulgation of FISA in 1978 (Savage 2014).

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 (*Al-Haramain Islamic Foundation Inc v Bush* 2007).

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 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" (*ACLU v NSA* 2007; *Hepting v AT&T* 2006; see Casey 2008, pp. 1020–1025).

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 plaintiffs 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 (*Clapper v Amnesty Intern USA* 2013).

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* (Savage 2013). This situation is now changing and the government has notified

some defendants in pending and final cases that they were subjected to the secret wiretapping (Savage 2013).

"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 (*Whitaker v Garcetti* 2003).

"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 (Schwartz 2008, p. 307).

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" (Schwartz 2008, p. 309).

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 (*United States v Truong Dinh Hung* 1980).

Even before 9–11, however, evidence legally gathered through a FISA wiretap could be used in a criminal prosecution against a US person (*United States v Duggan* 1984; *United States v Nicholson* 1997; *United States v Pelton* 1987; *United States v Sarkissian* 1988). 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 easier 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 (*United States v Ning Wen* 2006). 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 (*In re: Sealed Case* 2002).

Because of the more flexible rules for FISA wiretaps, metadata orders and NSLs, the bulk of which are acquired by NSA and FBI, lesser law enforcement entities, such as the Drug Enforcement Administration (DEA) seek to tailor their requests for wiretaps to fall within the categories of terrorism or national security, but the NSA is often reluctant to allow more conventional law enforcement agencies access to its huge archives of electronic metadata (Lichtblau and Schmidt 2013).

The Search for a New Paradigm

It is becoming clear to more scholars, judges, and the public in the USA, that the traditional 4.Amend. approach to privacy protection is obsolete in the digital age. Even before the revelations 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 (*United States v Jones* 2012a, b).

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 (Ghoshray 2012, pp. 82–85; McAllister 2012, pp. 499–500).

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. (see generally, Kerr 2012). 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 (supporting the "inside-outside" approach and rejecting the "Mosaic" approach see Kerr 2012, pp. 346–353).

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 (McAllister 2012, pp. 512–529; Slobogin 2008, pp. 333–336).

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" (Casey 2008, pp. 1030–1031).

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 suf-

fice 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 (Slobogin 2008, p. 337).

Slobogin differentiates between target-driven searches, 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 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 (Slobogin 2008, p. 338).

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 (Weisman 2013), 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 (Shane 2013d). Hopefully this means that changes may be on the way.

References

Adler, M. (1996). Cyberspace, general searches, and digital contraband: The fourth amendment and the net-wide search. *Yale Law Journal, 105*, 1093.

Apuzzo, M. (2014, March 19). Judge Rebukes Justice Dept. for Requesting Overly Broad E-Mail Searches. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2014/03/20/us/judge-rebukes-officials-over-requests-for-broad-email-searches.html?ref=us.

Automatic Number Plate Recognition. (2015). *Wikipedia*. Retrieved March 22, 2015, from http://en.wikipedia.org/wiki/Automatic_number_plate_recognition#United_States.

Bales, C. (2012). Unbreakable: The fifth amendment and computer passwords. *Arizona State Law Journal, 44*, 1293.

Brenner, S. (2012). Encryption, smart phones, and the fifth amendment. *Whittier Law Review, 33*, 525; 533–534.

Casey, T. (2008). Electronic surveillance and the right to be secure. *University of California Davis Law Review, 41*, 977.

Engel, J. (2012). Rethinking the application of the fifth amendment to passwords and encryption in the age of cloud computing. *Whittier Law Review, 33*, 543.

Fox, C. (2012). Checking in: Historic cell site location information and the stored communications act. *Seton Hall Law Review, 42*, 769.

Ghoshray, S. (2012). Looking through the prism of privacy and trespass: Smartphones and the fourth amendment. *University of the District of Columbia David A. Clarke School of Law Review, 16*, 73.

Glanz, J., Larson, J., & Lehren, A. W. (2014, January 27). Spy agencies tap data streaming from phone apps. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?ref=world&_r=0.

Goldstein, J. (2013, January 15). Police to use fake pill bottles to track drugstore thieves. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/01/16/nyregion/ny-police-to-track-drugstore-robbers-via-decoy-bottles.html.

Kerr, O. (2010). Applying the fourth amendment to the Internet: A general approach. *Stanford Law Review, 62*, 1005.

Kerr, O. (2012). The mosaic theory of the fourth amendment. *Michigan Law Review, 111*, 311.

Kimel, C. (2013). DNA profiles, computer searches, and the fourth amendment. *Duke Law Journal, 62*, 933.

Lichtblau, E., & Schmidt M. S. (2013, August 3). Other agencies clamor for data N.S.A. compiles. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/08/04/us/other-agencies-clamor-for-data-nsa-compiles.html?ref=us.

Lichtblau, E. (2005, April 5). Justice Dept. Defends Patriot Act Before Senate Hearings. *New York Times* (p. A21).

Mazzetti, M., & Elliot, J. (2013, December 9). Spies infiltrate a fantasy realm of online games. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html?ref=world.

McAllister, M. (2012). The fourth amendment and new technologies: The misapplication of analogical reasoning. *Southern Illinois University Law Journal, 36*, 475.

Miller, G., Tate, J., & Gellman, B. (2013, October 16). Documents reveal N.S.A.'s extensive involvement in targeted killing program. *Washington Post*. Retrieved July 9, 2015, from http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html.

Nixon, R. (2013, July 3). U.S. postal service logging all mail for law enforcement. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?ref=us.

Nixon, R. (2014, October 27). Report reveals wider tracking of mail in U.S. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2014/10/28/us/us-secretly-monitoring-mail-of-thousands.html?ref=us.

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. able to foil basic safeguards of privacy on web. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?ref=world.

Risen, J., & Lichtblau, E. (2013, June 8). How the U.S. uses technology to mine more data more quickly. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html?ref=world&_r=0.

Risen, J., & Poitras, L. (2014, May 31). N.S.A. collecting millions of faces from web images. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?ref=us.

Savage, C., & Baker, P. (2013, May 22). Obama, in a shift, to limit targets of drone strikes. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/05/23/us/us-acknowledges-killing-4-americans-in-drone-strikes.html?ref=us.

Savage, C., & Mazzetti, M. (2013, November 14). C.I.A. collects global data on transfers of money. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html.

Savage, C. (2013, July 25). Roberts's picks reshaping secret surveillance court. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/07/26/us/politics/robertss-picks-reshaping-secret-surveillance-court.html?ref=us.

Savage, C. (2014, June 17). Lawyer not entitled to see classified surveillance material court rules. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2014/06/18/us/lawyer-not-entitled-to-see-classified-surveillance-material-court-rules.html?ref=us.

Schwartz, P. (2008). Reviving telecommunications surveillance law. *University of Chicago Law Review, 75*, 287.

Sengupta, S. (2013a, February 15). Rise of drones in U.S. drives efforts to limit police use. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?ref=us&_r=0.

Sengupta, S. (2013b, October 13). Privacy fears grow as cities increase surveillance. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html?ref=us.
Shane, S. (2013a, April 7). Targeted killing comes to define war on terror. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/04/08/world/targeted-killing-comes-to-define-war-on-terror.html?ref=world&_r=0.
Shane, S. (2013b, February 8). Debating a court to vet drone strikes. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/02/09/world/a-court-to-vet-kill-lists.html?ref=us&_r=0.
Shane, S. (2013c, July 19). Surveillance court renews order for phone call data. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/07/20/us/surveillance-court-renews-order-for-phone-call-data.html?ref=us.
Shane, S. (2013d, July 25). Spy agencies under heaviest scrutiny since abuse scandal of the 70's. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/07/26/us/politics/challenges-to-us-intelligence-agencies-recall-senate-inquiry-of-70s.html?ref=us.
Slobogin, C. (2005). Transaction surveillance by the government. *Mississippi Law Journal, 75*, 139.
Slobogin, C. (2008). Government data mining and the fourth amendment. *University of Chicago Law Review, 75*, 317.
Sullivan, B. (2001, November 20). FBI software cracks encryption wall. *MSNBC*. Retrieved July 9, 2015, from http://www.nbcnews.com/id/3341694/#.UZCVKcrLsoE.
Thaman, S. C. (2001). Landesbericht U.S.A. In W. Gropp & B. Huber (Eds.), *Rechtliche Initiativen gegen organisierte Kriminalität*. Freiburg im Breisgau: Max-Planck-Institute for Foreign and International Comparative Law.
Weisman, J. (2013, July 24). House defeats effort to rein in N.S.A. data gathering. *New York Times*. Retrieved July 9, 2015, from http://www.nytimes.com/2013/07/25/us/politics/house-defeats-effort-to-rein-in-nsa-data-gathering.html?ref=us.
Worth, R. F., Mazzetti, M., & Shane, S. (2013, February 6). Hazards of drone strikes face rare public scrutiny. *New York Times* (p. A1, A10).

United States Court Cases

ACLU v. NSA, 493 F 3d 644, 655-57 (6th Cir 2007).
Al-Haramain Islamic Foundation Inc v Bush, 507 F 3d 1190, 1193 (9th Cir 2007).
Almada v State, 994 P 2d 299, 307-08 (Wyo 1999).
Andresen v Maryland, 427 US 463, 473 (1976).
Baird v State, 398 S W 3d 220, 230 (Tex Crim App 2013).
California Banker's Ass'n, 416 US 21, 53-54 (1974).
Clapper v. Amnesty Intern USA,133 S Ct 1138, 1148-49 (2013).
Commonwealth v Augustine, 4 N E 3d 846, 867 (Mass 2014).
Commonwealth v Bender, 811 A 2d 1016 (Pa Super 2002).
Commonwealth v Brion, 652 A 2d 287, 289 (Pa 1995).
Commonwealth v Efaw, 774 A 2d 735 (Pa 2001).
Commonwealth v Gelfgatt, 11 N E 3d 605, 615-16 (Mass 2014).
Commonwealth v Rousseau, 990 N E 2d 543, 551–53 (Mass 2013).
Cowles v State, 23 P 3d 1168, 1172 (Alaska 2001).
Devega v State, 689 S E 2d 293, 299–300 (Ga 2010).
Doe v United States, 487 US 201, 214–19 (1988).
Douglas v Dobbs, 419 F 3d 1097, 1102 (10th Cir 2005).
Fisher v United States, 425 US 391, 408 (1976).
Florida v Jardines, 133 S Ct 1409, 1416 (2013).

Frasier v State, 794 N E 2d 449, 465 (Ind App 2003).
Georgia v Randolph, 547 US 103, 109–23 (2006).
Guest v Leis, 255 F 3d 325, 335, 342 (6th Cir 2001).
Hedgepath v Commonwealth, 441 S W 3d 119, 130–31 (Ky 2014).
Hepting v AT&T, 439 F Supp 2d 974 (N D Cal 2006).
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).
In re Application of the United States for an Order 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, 564 (E D N Y 2005).
In re Application of the United States, 736 F Supp 2d 578, 579 (E D N Y 2010).
In re Application of the United States, 747 F Supp 2d 827, 846 (S D Tex 2010).
In re Application of the United States, 809 F Supp 2d 113, 116, 127 (E D N Y 2011).
In re Application of United States for Historical Cell Site Data, 724 F 3d 600, 610–12 (5th Cir 2013).
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, 312–13 (3d Cir 2010).
In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F 3d 1335, 1346, 1352–53 (11th Cir 2012).
In re Maxfield, 945 P 2d 196, 200–01 (Wash 1997).
In re Pers Restraint of Nichols, 256 P 3d 1131, 1135 (Wash 2001).
In re: Sealed Case No's 02-001, 02-002, 310 F 3d 717, 721 (USFIS App 2002).
Kyllo v United States, 533 US 27, 37 (2001).
Massachusetts v Sheppard, 468 US 981, 987–88 (1984).
People v Beavers, 227 N W 2d 511, 514 (Mich 1975).
People v Devone, 931 N E 2d 70, 74 (N Y 2010).
People v Gall, 30 P 3d 145, 153 (Colo 2011).
People v Harris, 886 N E 2d 947 (Ill 2008).
People v Mason, 989 P 2d 757, 760 (Colo 1999).
People v Nesbitt, 938 N E 2d 600, 605–06 (Ill App 2010).
People v Prinzing, 907 N.E.2d 87, 99–100 (Ill App 2009).
People v Stanley, 86 Cal Rptr 2d 89, 93 (Cal App 1999).
People v Weaver, 909 N E 2d 1195, 1199–1202 (N Y 2009).
Riley v. California, 134 S.Ct. 2473 (2014).
State v Augafa, 992 P 2d 723, 734 (Haw App 1999).
State v Boyd, 992 A 2d 1071, 1082–83 (Conn 2010).
State v Brereton, 826 N W 2d 369, 379 (Wis 2013).
State v Bridges, 925 P 2d 357 (Haw 1997).
State v Clark, 916 P 2d 384, 390 (Wash 1996).
State v Davis, 732 N W 2d 173, 182 (Minn 2007).
State v Domicz, 907 A 2d 395, 402–04 (N J 2006).
State v Earls, 70 A 3d 630, 645 (N J 2013).
State v Geraw, 795 A 2d 1219, 1225–26 (Vt 2002).
State v Glass, 583 P 2d 872, 875 (Alaska 1978).
State v Henderson, 854 N W 2d 616, 632–33 (Neb 2014).
State v Holden, 964 P 2d 318, 322 (Utah App 1998).
State v Jackson, 76 P 3d 217, 224 (Wash 2003).
State v Jordan, 156 P 3d 893, 898 (Wash 2007).
State v McAllister, 840 A 2d 967, 969 (N J App 2004).
State v Mubita, 188 P 3d 867, 875 (Idaho 2008).
State v Mullens, 650 S E 2d 169, 190 (W Va 2007).
State v Ortiz, 600 N W 2d 805, 817 (Neb 1999).

State v Page, 911 P 2d 513 (Alaska 1996).
State v Ruck, 155 Idaho 475, 484 (2013).
State v Rupnick, 125 P 3d 541, 547–48 (Kan 2005).
State v Russo, 790 A 2d 1132, 1140–41 (Conn 2002).
State v Skinner, 10 So 3d 1212, 1217–18 (La 2009).
State v Sloane, 939 A 2d 796, 803–04 (N J 2008).
State v Sobczak, 833 N W 2d 59, 71–73 (Wis 2013).
State v Subdiaz-Osorio, 849 N W 2d 748 (Wis 2014).
State v Tackitt, 67 P 3d 295, 302–03 (Mont 2003).
State v Wiegand, 645 N W 2d 125, 137 (Minn 2005).
State v Williams, 590 S E 2d 151, 154–55 (Ga App 2003).
State v Worthy, 661 A 2d 1244 (N J 1995).
State v Young, 867 P 2d 593 (Wash 1994).
State v Zahn, 812 N W 2d 490, 498 (S D 2012).
Stevenson v State, 667 So 2d 410, 411–12 (Fla App 1996).
Tracey v State, 152 So 3d 504, 524–26 (Fla 2014).
United States v Adjani, 452 F 3d 1140, 1150 (9th Cir 2006).
United States v Al-Marri, 230 F Supp 2d 535, 539–40 (S D N Y 2002).
United States v Andrus, 483 F 3d 711, 719–22 (10th Cir 2007).
United States v Biasucci, 786 F 2d 504, 510–11 (2d Cir 1986).
United States v Boyce, 351 F 3d 1102, 1107, 1111 (11th Cir 2003).
United States v Bradley, 644 F 3d 1213, 1259–61 (11th Cir 2011).
United States v Bridges, 344 F 3d 1010, 1016 (9th Cir 2003).
United States v Carey, 172 F 3d 1268, 1273 (10th Cir 1999).
United States v Christie, 717 F 3d 1156, 1164–66 (10th Cir 2013).
United States v Comprehensive Drug Testing, Inc, 621 F 3d 1162, 1171–72 (9th Cir 2010).
United States v Coreas, 419 F 3d 151, 157–59 (2d Cir 2005).
United States v Cuevas-Sanchez, 821 F 2d 248, 252 (5th Cir 1987).
United States v Davis, 326 F 3d 361, 365–66 (2d Cir 2003).
United States v Davis, 754 F 3d 1205, 1217 (2014).
United States v Doe, 465 US 605, 612–14 (1984).
United States v Duggan, 743 F 2d 59, 78 (2d Cir 1984).
United States v Falls, 34 F 3d 674, 680 (8th Cir 1994).
United States v Fernandez, 600 F3d 56 (1st Cir 2010).
United States v Forest, 355 F 3d 942, 950–51 (6th Cir 2004).
United States v Forrester, 512 F 3d 500, 509–11 (9th Cir 2008).
United States v Frechette, 583 F 3d 374, 379 (6th Cir 2009).
United States v Fricosu, 841 F Supp 2d 1232, 1237 (D Colo 2012).
United States v Garcia, 474 F 3d 994 (7th Cir 2007).
United States v Gonzalez, 328 F 3d 543, 548 (9th Cir 2003).
United States v Gourde, 440 F 3d 1065, 1071 (9th Cir 2006).
United States v Hambrick, 55 F Supp 2d 504, 508 (W D Va 1999).
United States v Heatley, 41 F Supp 2d 284 (S D N Y 1999).
United States v Hill, 459 F 3d 966, 975–77 (9th Cir 2006).
United States v Hill, 459 F 3d 966, 978 (9th Cir 2006).
United States v Hubbell, 530 US 27, 43 (2000).
United States v Jones, 132 S Ct 945, 946 (2012).
United States v Jones, 132 S Ct 945, 957 (2012).
United States v Karo, 468 US 705, 714–18 (1984).
United States v Kattaria, 503 F 3d 703, 707 (8th Cir 2007).
United States v Kennedy, 81 F Supp 2d 1103, 1110 (D Kan 2000).
United States v King, 604 F 3d 125, 134–37 (3d Cir 2010).
United States v Kirschner, 823 F Supp 2d 665, 668–69 (E D Mich 2010).
United States v Knotts, 460 US 276, 282 (1983).
United States v Kouzmine, 921 F Supp 1131, 1135 (S D N Y 1996).

United States v Koyomejian, 970 F 2d 536, 542 (9th Cir 1992).
United States v Lee, 359 F 3d 194, 199–203 (3d Cir 2004).
United States v Longoria, 177 F 3d 1179, 1183–84 (10th Cir 1999).
United States v Lucas, 640 F 3d 168, 177–78 (6th Cir 2011).
United States v Mann, 592 F 3d 779, 785 (7th Cir 2010).
United States v Martin, 426 F 3d 68, 74–75 (2d Cir 2005).
United States v Maynard, 615 F 3d 544, 560–63 (D C Cir 2010).
United States v McArthur, 573 F 3d 608, 613 (8th Cir 2009).
United States v Meriwether, 917 F 2d 955, 959 (6th Cir 1990).
United States v Mesa-Rincon, 911 F 2d 1433, 1437 (10th Cir 1990).
United States v Miller, 425 US 435, 442 (1976).
United States v Myers, 692 F 2d 823, 859 (2d Cir 1982).
United States v Nicholson, 955 F Supp 588, 590–93 (E D Va 1997).
United States v Ning Wen, 471 F 3d 777 (7th Cir 2006).
United States v Padilla, 520 F 2d 526, 528 (1st Cir 1975).
United States v Paxton, 573 F 3d 859, 861–62 (9th Cir 2009).
United States v Pelton, 835 F 2d 1067, 1075–76 (4th Cir 1987).
United States v Purcell, 236 F 3d 1274, 1279 (11th Cir 2001).
United States v Reyes, 922 F Supp 818, 833–34 (S D N Y 1996).
United States v Richards, 659 F 3d 527, 539–40 (6th Cir 2011).
United States v Sarkissian, 841 F 2d 959, 965 (9th Cir 1988).
United States v Scarfo, 180 F Supp 2d 572, 578 (D N J 2001).
United States v Shields, 458 F 3d 269, 278 (3d Cir 2006).
United States v Thomas, 757 F2d 1359, 1367 (2d Cir 1985).
United States v Torres, 751 F 2d 875, 880–82 (7th Cir 1984).
United States v Truong Dinh Hung, 629 F 2d 908 (4th Cir 1980).
United States v Turner, 169 F 3d 84, 88–89 (1st Cir 1999).
United States v Upham, 168 F 3d 532, 535 (1st Cir 1999).
United States v Vankesteren, 553 F 3d 286, 290–91 (4th Cir 2009).
United States v Villegas, 899 F 2d 1324, 1335–36 (2d Cir 1990).
United States v Wagers, 452 F 3d 534, 542–43 (6th Cir 2006).
United States v Wahchumwah, 704 F 3d 606 (9th Cir 2012).
United States v White, 401 US 745, 749–51, 762–63, Douglas dissent at 756, Harlan dissent at 786 (1971).
United States v Williams, 124 F 3d 411, 417 (3d Cir 1997).
United States v Williams, 592 F 3d 511, 521–24 (4th Cir 2010).
United States v Yonn, 702 F 2d 1341, 1347 (11th Cir 1983).
United States v Ziegler, 474 F 3d 1184, 1191–92 (9th Cir 2007).
US v Giberson, 527 F 3d 882, 889–90 (9th Cir 2008).
Whitaker v Garcetti, 291 F Supp 2d 1132, 1138 (C D Cal 2003).

United States Statutes

§ 213 US PATRIOT Act
12 USC § 3410–22.
18 USC § 2705(a)(2).
18 USC § 3103(a).
18 USC §§ 2701–12.
50 USC § 1825(b).
50 USC §§ 1822–24.
Pub L 91-508, 84 Stat 1114 (1970).