Richmond Journal of Law and Technology

Volume 13 | Issue 1 Article 4

2006

Double-Trouble: The Underregulation Of Surreptitious Video Surveillance In Conjunction With The Use Of Snitches In Domestic Government Investigations

Mona R. Shokrai
mona.shokrai@gmail.com

DOUBLE-TROUBLE: THE UNDERREGULATION OF SURREPTITIOUS VIDEO SURVEILLANCE IN CONJUNCTION WITH THE USE OF SNITCHES IN DOMESTIC GOVERNMENT INVESTIGATIONS

*Mona R. Shokrai**

[1] Technological advancements in digital imagery and visual recordings have all but vitiated any expectation of privacy in public places. Yet this Orwellian state of constant governmental surveillance has extended beyond the scope of public observation. Closely-held expectations of privacy in the most intimate locations have also become subject to government observation. The means by which the government is able to garner such detailed information concerning the minutiae of our private lives is in need of assessment.

[2] Covert video surveillance is one of the most intrusive mechanisms by which law enforcement officials can gather incriminating evidence. The invasiveness of this investigative technique requires that some kind of procedural safeguards be applied in order to protect our fundamental interests against government searches and seizures under the Fourth Amendment.[1] However, there are currently no guidelines in place to regulate domestic investigations utilizing any form of video surveillance. Protective doctrines such as the warrant requirement and its procedural

*J.D., Loyola Law School, Los Angeles, 2006. Mona.Shokrai@gmail.com. The issues raised in this Article stemmed from my legal work with Richard G. Novak, Esq., to whom I am indelibly grateful for providing me with the knowledge and excitement to write about this gap in the law. Many thanks to Gina Genova, Mariana Mello, Natalie Artin, Professor Susan Bakhshian, and Professor Gary Marx for their thoughts and assistance. Special thanks to Professor Alexandra Natapoff for her guidance and feedback throughout the process—and for being impressed with my "willingness to try hard things." A very special thank you to Amir Aharonov who contributed countless hours of his insight, hard critique, and brilliance.

[1] U.S. CONST. amend. IV.

hurdles protect our rights against government intrusion in private locations. When these procedural safeguards are circumvented, our constitutional rights become placed in jeopardy of governmental violation.

[3] Despite the lack of specific regulation for video surveillance, many courts have applied provisions of related doctrines, such as the law governing wiretapping and electronic surveillance,[2] to this type of investigation. When surreptitious video surveillance is carried out in conjunction with the use of consenting informants, a regulatory loophole is created that can result in unjustified governmental intrusions upon the rights of the surveillee. The confluence of these two areas of jurisprudence creates a path by which law enforcement officials are able to effectively bypass the warrant requirement or any other applicable procedural hurdle. Without creating specifically tailored legislation or precedent to govern investigations utilizing snitches to surreptitiously videotape the subjects of an investigation, the police need only find an accomplice to circumvent all constitutional protections.[3]

[4] This paper discusses this problem in current regulation and the implications of this regulatory inconsistency. Part I discusses the law governing domestic video surveillance under its current judicial permutations. It also illustrates the inconsistency in application by looking at a jurisdictional survey of case law on the topic. Part II discusses the current law governing the use of snitches in undercover investigations, the effects of which have created the regulatory loophole at issue. Part III then discusses the institutional, social, and regulatory ramifications of allowing such regulatory inconsistencies to persist.

I. CURRENT LAW GOVERNING VIDEO SURVEILLANCE

[5] The pervasiveness of video cameras and other visual recording devices in daily life supports the need for regulations and parameters in place to govern their uses.[4] The amount of detail that can be garnered from video

[2] *See e.g.* 18 U.S.C. §§ 2510–2518 (2001).
[3] *See* Melanie L. Black Dubis, *The Consensual Electronic Surveillance Experiment: State Courts React to United States v. White*, 47 VAND L. REV. 857 (1994).
[4] *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 405 (1997). The author states that the ABA's definition of video surveillance excludes "the

surveillance recordings underscores the necessity for applicable guidelines.[5] There is no single rule in application that regulates various forms of video surveillance and recording in both the public and private spheres. While public locations are considered "fair game"[6] as the subject of virtually any method of surveillance under the doctrine of public exposure,[7]the most significant deficiencies in regulation arise from covert, hidden, or surreptitious video surveillance[8] of private locations.[9]

A. SURREPTITIOUS VIDEO SURVEILLANCE PROMPTS A HIKE IN THE LEVEL OF INTRUSION UPON THE PRIVACY INTEREST OF THE SURVEILLEE

[6] Advancements in surveillance technology have supplied law enforcement with numerous new investigative tools, tactics, and methods. These advancements have been the source of tremendous simplification and ease, providing investigators with time and effort saving advantages to more traditional painstaking investigative tactics.[10] Nonetheless, these advances have simultaneously created the prospect of colossal invasions into individual privacy.[11] Video camera surveillance is distinguishable

use of a 'lawfully positioned' camera to view or record activities 'occurring within the sight or immediate vicinity of a law enforcement official (or agent thereof) who is aware of such use.'" *Id.* at 414.

[5] *Id.* at 385-408.

[6] This refers to the lack of any expectation of privacy an individual is held to retain, and the consequential authority vested in the surveillors to implement such surveillance without having to stay within any defined boundaries.

[7] The Fourth Amendment does not protect what one knowingly exposes to the public. Information, actions, and conduct that are "knowingly exposed to the public" are considered to be in plain view. Consequently, capturing or viewing this content by any method of surveillance, is not defined as a "search" under the ambit of Fourth Amendment protection. In contrast, Constitutional protection extends to that which one keeps private (even within a public location). *See* Katz v. United States, 389 U.S. 347, 351 (1967).

[8] *See* Slobogin, *supra* note 4, at 414. Professor Christopher Slobogin clarifies the determination for covert surveillance by including whether the law enforcement surveyor "intends that the subject of the surveillance be unaware of the monitoring and if a reasonable person in the subject's position would be unaware of it." *Id.* at 414-15.

[9] The focus of this paper is on covert video surveillance that is conducted in private locations. Public or overt video surveillance, which carry independent concerns under the realm of Fourth Amendment analysis, are not within the scope of this paper.

[10] *See* Ric Simmons, *Symposium: The Powers and Pitfalls of Technology: Technology-Enhanced Surveillance By Law Enforcement Officials*, 60 N.Y.U. ANN. SURV. AM. L. 711 (2005).

[11] *Id.* at 711.

from traditional physical searches.[12] Because of this prospect, our society should focus less on investigative efficiency, and more on the need to reinforce and safeguard our Fourth Amendment rights with more vigor.

[7] In *Lopez v. United States*, the United States Supreme Court established that the use of technology adds no greater intrusion to a search.[13] However, the nuances of video surveillance distinguish it from the oral or wire communications the Court discusses in *Lopez*. Physical searches, or even aural surveillance and recordation, do not reach the level of invasiveness that is the product of visual surveillance and recordation. The minutiae or peripheral imagery captured, oftentimes containing visual cues beyond the line of sight of any cooperating informant or party to the conversation, can be reviewed, enlarged, or even enhanced to provide the investigating agents with evidence they would not have been able to acquire by any other means.[14] No debriefing or testimony provided by an informant or party to the conversation would be able to match the fine details or imagery depicted and acquired by a video recording.[15]

[8] Federal appellate courts visiting this issue have also characterized surreptitious video surveillance as "one of the most intrusive investigative

---

[12] *See* GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 217-19 (1988). In his book on covert police action, Professor Marx notes ten characteristics of new investigative technologies "that set them apart from most traditional forms of social control":

(1) The new surveillance transcends distance, darkness, and physical barriers;
(2) It transcends time; its records can be stored, retrieved, combined, analyzed, and communicated;
(3) It has low visibility or is invisible;
(4) It is often involuntary;
(5) Prevention is a major concern;
(6) It is capital- rather than labor-intensive;
(7) It involves decentralized self-policing;
(8) It triggers a shift from targeting a specific suspect to category suspicion of everyone (or at least everyone within a particular category);
(9) It is more intensive; and
(10) It is more extensive.

[13] Lopez v. United States, 373 U.S. 427 (1963).

[14] *See* Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDIS. L.J. 295, 309-11 (1999).

[15] United States v. Davis, 326 F.3d 361, 367 (S.D.N.Y 2003); Lopez, 373 U.S. at 439.

mechanisms available to law enforcement."[16] In particular, the Ninth Circuit has acknowledged and integrated this description of hidden video surveillance in its interpretations and in its rulings on several cases involving covert visual recording and surveillance during criminal investigations. Because of its invasiveness, video surveillance has been found to reach "beyond the perimeter of a person's reasonable expectations of privacy"—far beyond the scope of other electronic monitoring devices.[17] The Ninth Circuit further noted, "[t]he silent, unblinking lens of the camera was intrusive in a way that no temporary search of [a home or] office could have been."[18]

[9] In *United States v. Nerber*, the Ninth Circuit noted, "[t]he sweeping, indiscriminate manner in which video surveillance can intrude upon us, regardless of where we are, dictates that its use be approved only in limited circumstances."[19] Further, Judge Kozinski of the Ninth Circuit, visiting the issue of regulating video surveillance in his concurrence in *United States v. Koyomejian*, articulated:

> As every court considering the issue has noted, video surveillance can result in extraordinarily serious intrusions into personal privacy. Is it reasonable to place a camera in the home where it is likely to monitor people while they go to the bathroom, while they engage in intimate relations, while they cook and clean, while they sweep dirt under the rug? If such intrusions are ever permissible, they must be justified by an extraordinary showing of need.[20]

[10] Since courts consider video surveillance an immense intrusion into personal privacy, our society must be concerned with the current state of regulatory limbo. Despite the need for a universally applicable set of guidelines controlling the use of video surveillance, there is more room for irregularity because jurisdictionally-specific approaches currently govern this process.

---

[16] United States v. Nerber, 222 F.3d 597, 603 (9th Cir. 2000).
[17] United States v. Andonian, 735 F.Supp. 1469,1478 (9th Cir. 1990).
[18] United States v. Taketa, 923 F.2d 665, 677 (9th Cir. 1991).
[19] Nerber, 222 F.3d at 603.
[20] United States v. Koyomejian, 970 F.2d 536, 551 (9th Cir. 1992) (Kozinski, J., concurring).

B. DISTINCT JURISPRUDENTIAL APPROACHES TO COVERT VIDEO SURVEILLANCE

[11] Circuit courts facing the issue of covert, surreptitious video surveillance from within private locations have applied various approaches – some courts drawing on existing criminal jurisprudence for analysis, while other courts have failed to articulate any approach. Commonality between some circuits can only be found in application of two main branches of criminal jurisprudence to this inquiry: (1) Analysis under the Fourth Amendment,[21] and (2) The application of Title III's regulations governing "electronic communications."[22] Of those circuits that have ventured to create an analytical framework, some circuits have drawn on the former exclusively, others exclusively on the latter, while even other circuits have taken this analysis beyond the bounds of these two approaches by uniquely hybridizing these two doctrines into a more narrow approach toward video surveillance. Regardless of which approach a court decides to apply, however, the current state of regulation is still unclear.

1. ANALYSIS OF THE FOURTH AMENDMENT TO THE CONSTITUTION

[12] The foundational issue in any Fourth Amendment analysis is whether a search or seizure has taken place.[23] This determination depends on whether the subject of the search, in this case the individual being surveilled, had a reasonable expectation of privacy in the locale at issue.[24] But what constitutes a reasonable expectation of privacy? Courts have been grappling with this issue in various contexts for quite some time.

[13] Justice Harlan's concurring opinion in *Katz v. United States*[25] provided the benchmark standard from which to analyze whether the subject of a search had a reasonable expectation of privacy. A legally cognizable expectation of privacy must not only objectively be one that society is prepared to recognize as reasonable, but the individual being

[21] U.S. CONST. amend. IV.
[22] 18 U.S.C. §§ 2510-2522 (2001).
[23] Slobogin, supra note 4 at 389.
[24] Katz v. United States, 389 U.S. 347, 351 (1967).
[25] *Id*.

searched must also have a subjective expectation of privacy in that particular encounter.[26]

[14] The traditional inquiry often involves some sort of physical intrusion that implicates this analysis.[27] However, covert video surveillance often fails to generate any form of physical contact. Nonetheless, the Fourth Amendment's guarantee against unreasonable searches does not retreat simply because no physical intrusion has transpired.[28]

[15] The intrusion effected by the common physical search[29] is terminated at the conclusion of the encounter; the subject of this search will generally be confident that all such contact has ceased. In contrast, the subject of video surveillance can never be certain that an encounter is taking place, and if so, at what point it has terminated,[30] rendering video searches more intrusive and of a nature that may be characterized as one that society is prepared to recognize as objectively unreasonable. As long as the subject of the video surveillance can demonstrate a subjective expectation of privacy in the subject of the surveillance, the surveillee may maintain a *Katz* claim that he or she did have a reasonable expectation of privacy, notwithstanding the lack of any physical intrusion or contact during the encounter.[31]

---

[26] *Id.* at 361.

[27] *Id.* at 352-53.

[28] *Id.*

> It is true that the absence of [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry . . . for that amendment was thought to limit only searches and seizures of tangible property. But the premise that property interests control the right of the Government to search and seizure has been discredited.

Id. (citing Warden v. Hayden, 387 U.S. 294, 304 (1967)).

[29] Primitive searches refer to those generating physical contact between the law enforcement agent and the subject of the search. Common examples include a pat-down on the subject's person, or the search of closed cabinets within a private dwelling.

[30] *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1355-56 (2004).

[31] Katz v. United States, 389 U.S. 347, 351 (1967). *Katz* involved no physical intrusion, yet the court recognized that the defendant did maintain a reasonable expectation of privacy and as such, his Fourth Amendment rights were maintained.

[16] When faced with the issue of admissibility of evidence acquired through video surveillance, the Tenth Circuit in *United States v. Mesa-Rincon* noted, "[t]he Fourth Amendment protects us against 'unreasonable searches and seizures.' To determine whether a search is 'reasonable,' we must balance the intrusiveness of the method used and the expectation of privacy in the premises searched with the government's showing of necessity for the search."[32] In order to fairly scrutinize the regulation of surreptitious video surveillance, these conflicting interests must be evaluated. From a law enforcement perspective, video surveillance not only enhances investigative capabilities, but also prompts a sharp decrease in the strain on investigative resources. Despite such countervailing benefits to state interests, use of covert video surveillance as an investigative tool engenders a plethora of consequences, causing severe detriment to the interests of the individual.[33]

[17] The impetus for constructing the warrant requirement, as found in the language and composition of the Fourth Amendment, was to safeguard the individual from any unjustifiable intrusion, either generated by the search itself or as a byproduct of a proper search.[34] Beyond the elemental

[32] United States v. Mesa-Rincon, 911 F.2d 1433, 1442 (10th Cir. 1990). *See also*, Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 5 (1991). In his article, Professor Slobogin notes, "As American courts have recognized, the regulation of search and seizure involves balancing the conflicting state and individual interests implicated by the investigative process." *Id.* at 5. As video surveillance and other technologically advanced investigative tools streamline the process of gathering evidence, we are left only with the Fourth Amendment to protect our privacy rights and expectations. In characterizing the regulation of a search carried out through video surveillance, we must first consider this balancing—between the usefulness of video surveillance for the state's investigations, and the intrusiveness of video surveillance upon the individual's privacy.

[33] Steagald v. United States, 451 U.S. 204, 222 (1981)

> [I]n those situations in which a search warrant is necessary, the inconvenience incurred by the police is generally insignificant. Whatever practical problems [there are in requiring a search warrant]…they cannot outweigh the constitutional interest at stake in protecting the right of presumptively innocent people to be secure in their homes from unjustified, forcible intrusions by the government.

[34] U.S. Const. amend. IV

> 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

probable cause requirement,[35] law enforcement agents must obtain a warrant prior to initiating a search. The warrant requirement compels investigators to seek ex ante authorization from a neutral and detached judicial officer before properly initiating a search.[36] Warrantless searches are per se unconstitutional under the Fourth Amendment. However, if the encounter falls within one of the recognized exceptions to the warrant requirement,[37] most of which are based on principles of exigency, a warrantless search may be permissible. If none of these exceptions apply and a search is carried out without a warrant, the subject of the search has a viable claim for the suppression of any evidence gathered or fruits derived therefrom.[38]

[18] Additional constraints emerge from the particularity requirement, effectively limiting the scope of an investigation. The Supreme Court in *Berger v. New York*[39] visited the need for such particularity, especially in the context of eavesdropping:

> The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on

---

> or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[35] Although there are various situations where probable cause is not required, the issues that arise within the scope of this paper are not applied to such situations.

[36] Steagald v. United States, 451 U.S. 212, 214 (1981) ("Absent exigent circumstances, a magistrate, rather than a police officer, must make the decision that probable cause exists to believe that person or object to be seized is within a particular place.").

[37] When there is an applicable exception to the warrant requirement, the law enforcement officials do not need to obtain a warrant before initiating the search because the circumstances at issue validate the search and the use of evidence found therein. The exceptions are fact-specific and oftentimes complex, but generally arise in the following circumstances: (i) when there are exigent circumstances, (ii) an item is in plain view, (iii) the search involves a mobile automobile, (iv) the search is incident to the subject's arrest, (v) the subject consented to the search, (vi) the search is within a 'sensitive area' (such as an airport or border), or (vii) the search is cursory and only requires reasonable suspicion. *See* State v. Hendrickson, 129 Wn.2d 61, 71, 917 P.2d 563, 572 (Wash. 1996) (citing Robert F. Utter, *Survey of Washington Search and Seizure Law: 1988 Update*, 73 U. PUGET SOUND L. REV. 411, 528-80 (1988)).

[38] Slobogin, *supra* note 4 at 449.

[39] Berger v. New York, 388 U.S. 41, 56 (1967).

> privacy that is broad in scope. As was said in *Osborn v. United States*[40], the 'indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments,' and imposes 'heavier responsibility on this Court in its supervision of the fairness of procedures.'[41]

The Court went on to discuss how a lack of such particularity, in effect, bypasses the purpose and rationale of the probable cause requirement:

> The Fourth Amendment's requirement that a warrant 'particularly describ[e] the place to be searched, and the persons or things to be seized,' repudiate[s] general warrants and 'makes general searches…impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.[42]

Insofar as these obstacles are in place and a warrant is properly executed, a higher probability of the integrity of the search is maintained.[43]

[19] If the video surveillance is conducted either pursuant to a properly executed warrant or without a warrant but properly justified by one of the recognized exceptions, video surveillance is permitted and admissible against the surveillee. Courts analyzing investigations utilizing surreptitious video surveillance have generally rejected claims that its inherent intrusiveness makes it per se unconstitutional under the Fourth Amendment.[44]

---

[40] Osborn v. United States, 385 U.S. 323, 329 n.7 (1966).
[41] Berger, 388 U.S. at 56.
[42] *Id.* at 58-59.
[43] It should also be noted that while the *Berger* Court recognized this necessity in the general context of eavesdropping, it follows that such particularity is even more vital when dealing with hyper-intrusive eavesdropping techniques such as covert video surveillance.
[44] *See e.g.* United States v. Taketa, 923 F.2d 665 (9th Cir. 1991); United States v. Andonian, 735 F. Supp. 1469, 1478 (C.D. Cal 1990); United States v. Gonzalez, 328 F.3d 543 (9th Cir. 2003); United States v. Shryock, 342 F.3d 948, 978 (9th Cir. 2003); United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

2. APPLICATION OF TITLE III TO VIDEO SURVEILLANCE

[20] When enacted in 1968, the drafters of Title III of the Omnibus Crime Control and Safe Streets Act of 1968[45] purported to create a more efficient regulatory framework for controlling wiretaps, bugging devices, and other similar aural surveillance methods. They aimed to create strict and narrow prerequisites that were difficult to meet, in an effort to justify the increased level of intrusion upon an individual's personal privacy.[46] While Title III does not expressly address video surveillance, courts occasionally apply its designation of "electronic communications"[47] in cases involving video surveillance investigations.[48]

[21] First and foremost, Title III imposes a probable cause requirement, analogous to that found under the prescriptions of the Fourth Amendment.[49] Without demonstrating probable cause to support the investigator's belief that the subject of the impending investigation "has committed, is committing, or is about to commit a particular offense"[50] and that surveying such communications will provide evidence of this commission,[51] the agent seeking judicial authorization under Title III should be unsuccessful.

[22] In addition to this preliminary showing, Title III's procedural regulations mandate that each application for a wiretap include facts sufficient for the reviewing judge to conclude, "normal investigative

[45] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2520 (2001)).

[46] *Id.*

> (d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused.

[47] 18 U.S.C. § 2510 (2001).

[48] *Id*.

[49] 18 U.S.C. § 2511 (2001).

[50] 18 U.S.C. § 2518(3)(a) (2001).

[51] 18 U.S.C. § 2518(3)(b).

procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[52] This prong can be met via a convincing argument from the investigating officer that other methods would be unavailing. Rationale for the existence of this particular requirement is based on the desire to strictly limit the use of wiretaps and ensure that it is not resorted to in situations where "traditional investigative measures"[53] would suffice to expose the crime.[54] Absent specific circumstances that render normal investigative techniques particularly ineffective, the application must be denied.[55]

[23] The next statutory constraint requiring a high degree of specificity for the purported allegations is akin to the particularity requirement of the Fourth Amendment.[56] In the same vein as warrant requirement logic, Title III requires a showing of particularity of the places to be searched and items to be seized in the application's endorsement of necessity.[57]

[24] In an effort to prevent abuses of this potentially harmful privilege, Section 2518(5) of Title III additionally requires a degree of minimization during the period of interception.[58] Without this constraint, the law enforcement officials conducting the interception would have almost limitless access to their subjects' private conversations. As a result, these investigators may improperly be exposed to incriminating evidence that they were not otherwise privy to. By further adding a thirty-day limitation on the period of judicially authorized interception, the drafters of Title III recognized its high potential for abuse.[59]

---

[52] S. REP. NO. 1097, at 101 (1968) ("Normal investigative procedure would include, for example, standard visual or aural surveillance techniques by law enforcement officers, general questioning or interrogation under an immunity grant, use of regular search warrants, and the infiltration of conspiratorial groups by undercover agents or informants...").
[53] United States v. Commito, 918 F.2d 95, 98 (9th Cir. 1990).
[54] *See e.g.* United States v. Kahn, 415 U.S. 143, 152 (1974); United States v. Brown, 761 F.2d 1272 (9th Cir. 1985); Commito, 918 F.2d at 98; United States v. Smith, 893 F.2d 1573, 1582 (9th Cir. 1990).
[55] *See* United States v. Ippolito, 774 F.2d 1482, 1486 (9th Cir. 1985).
[56] 18 U.S.C. § 2518(4) (2001).
[57] *Id.*
[58] 18 U.S.C. § 2518(5) (2001).
[59] *Id.*

[25] The remedy for a violation of the wiretap's procedural regulations is suppression. Section 2518(10)(a) of the federal wiretap statute provides in pertinent part, "Any aggrieved person in any trial . . . before any court . . . may move to suppress the contents of any wire or oral communication intercepted . . . or evidence derived therefrom, on the grounds that . . . the order of authorization or approval under which it was intercepted is insufficient on its face."[60] Essentially, if the affidavit fails to satisfy the necessity requirement or is procedurally defective in some way, the reviewing court is expected to suppress the communications at issue in order to safeguard the privacy interests of the parties to the interception.

[26] In 1968, when Title III[61] was passed, video technology had just begun to emerge as an investigative tool.[62] As such, there was little chance that such a budding development would have specific reference in the statute. Despite the fact that the technology for video surveillance—and even surreptitious video surveillance—has been widely available to the general public for quite some time,[63] both the courts and our legislative bodies have failed to affirmatively regulate this area. Peculiarly, a great deal of particularized attention has been placed upon the regulation of aural surveillance and other types of electronic communications, while visual surveillance has been all but ignored. As the rationale for implementing these regulations on aural and electronic surveillance is based mainly upon the need to normalize investigative methods that are so frequently utilized, it is unclear why visual surveillance (which is also used quite frequently) has not been similarly regulated.

[27] Future amendments to Title III fail to shed any light on the intended regulation of video surveillance or recordings. The Electronic Communications Privacy Act of 1986 ("ECPA")[64] amended Title III to

[60] 18 U.S.C. § 2518(10)(a)(ii) (2001).
[61] 18 U.S.C. §§ 2510-2520 (2001).
[62] *See generally* Robert C. Owen and Melissa Mather, *The Decisionmaking Process: Thawing Out the "Cold Record": Some Thoughts on How Videotaped Records May Affect Traditional Standards of Deference on Direct and Collateral Review*, 2 J. APP. PRAC. & PROCESS 411 (2000).
[63] Miniaturized cameras for "discreet / unobtrusive surveillance" are inexpensive and publicly available for commercial use. *See* http://www.wecusurveillance.com/page/435746.
[64] 18 U.S.C. §§ 2510-2522. Congress renamed Title III as the "Electronic Communications Privacy Act of 1986," which is the amendment of the 1968 statute.

include the interception of electronic communications. In fact, Congress explicitly stated that the ECPA was not meant to include video surveillance. In the Senate Judiciary Committee Report accompanying the ECPA, the Committee reaffirmed the statutory definition of 'aural acquisition' and went on to clarify that "[o]ther forms of surveillance are not within the proposed legislation."[65] Judge Kozinski of the Ninth Circuit visited the issue of the omission of video surveillance from the amendments to Title III and posited,

> Does it really follow that, had Congress considered the matter directly, it would have treated video surveillance exactly the same as those methods it did consider? I find it more plausible to infer that by choosing to exclude video surveillance . . . Congress and the President were recognizing that it is different from wiretapping and should not be treated as the same.[66]

[28] In the interim, however, law enforcement officials are making use of these new technologies without express regulations to follow. Ultimately, the judiciary is left to regulate these matters, as defendants move to suppress the resulting evidence.[67]

3. HYBRID APPROACH TO VIDEO SURVEILLANCE RECORDINGS

[29] As there is no statute applicable to domestic recordings produced via surreptitious video surveillance, courts facing this issue have been developing creative ways to adjudicate it. Most notably, various courts have bifurcated the evidence itself, separating the evidence into the audio-only component and the silent video component, before determining its

---

[65] S. REP. NO. 1097, at 90 (1968); s*ee also* United States v. Torres, 751 F.2d 875, 886 (7th Cir. 1984); Simmons, *supra* note 10, at 733, n46.

[66] United States v. Koyomejian, 970 F.2d 536, 551 (9th Cir. 1992).

[67] *Id.* at 551

> By rushing to develop a code that will comprehensively deal with video warrants on its first outing in the field, my colleagues have overreached. Attempting the task normally reserved to the political branches, they have abdicated the adjudicatory function while undertaking the task of legislation badly. The result is that they have shackled the government with more restrictions than the Constitution imposes, while at the same time giving citizens less protection than the Constitution affords them.

admissibility.[68] The reviewing courts will then apply Title III to the audio-only component, while leaving the admissibility of the silent video component contingent on satisfaction of the Fourth Amendment requirements.[69]

[30] Despite the logic of this analytical approach, the inconsistency promulgated by these alternative methods of interpretation is becoming problematic. Without a generally applicable framework, subjects of video surveillance are held only to the judicial standards found in their jurisdiction while individual privacy protections and the admissibility of such evidence can differ from circuit to circuit.

C. JURISDICTIONAL SURVEY OF CASE LAW DEALING WITH VIDEO SURVEILLANCE

[31] Despite judicial recognition that this video surveillance does carry tendencies of heightened intrusiveness, the courts have generally found this level of intrusion to remain permissible under certain jurisdictionally specific guidelines. Yet, we are left with inconsistency, regardless of which approach a lower court chooses to apply.

1. SUPREME COURT

[32] The Supreme Court's analysis of electronic surveillance in several cases has provided us with a barebones regulatory scheme that many lower courts have applied to more specific methods of investigation.[70] Despite the statutory omission, many lower courts have made attempts to force the video surveillance square peg into the general electronic surveillance round hole.[71]

---

[68] *See e.g.* United States v. Shryock, 342 F.3d 948, 978 (9th Cir. 2003); *see also*, United States v. Honken, 378 F. Supp.2d 880 (8th Cir. 2004); United States v. Gonzalez, Inc., 412 F.3d 1102 (9th Cir. 2005); United States v. Fernandez, 388 F.3d 1199 (9th Cir. 2004); United States v. Smith, 413 F.3d 1253 (10th Cir. 2005).

[69] Shryock, 342 F.3d at 978. Audio portions of the recording fall under the ambit of Title III and will be admitted or suppressed based on that analysis. Then a separate analysis based on Fourth Amendment principles governs the silent visual recordings captured.

[70] *See* Mulligan, *supra*, note 14 at 315-17.

[71] *See* Kanya A. Bennett, Comment, *Can Facial Recognition Technology be used to Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition*

[33] In the 1967 case of *Berger v. New York,*[72] the Supreme Court recognized that certain methods of investigation produce greater invasions on individual privacy and autonomy than the classic physical search. The subject of *Berger* was the regulation of government-initiated "electronic eavesdropping"[73] in a New York statute. The state statute required the government investigator to present, under oath, a statement that provides:

> [T]hat there is reasonable ground to believe that evidence of a crime may be thus obtained, and particularly describing the person or persons whose communications, conversations or discussions are to be overheard or recorded and the purpose thereof . . . [and] in connection with the issuance of such an order the justice or judge … shall satisfy himself of the existence of reasonable grounds for the granting of such an application.[74]

The Court held that this statute was in violation of the Fourth Amendment, as it did not meet the threshold prescriptions of the warrant requirement.[75] "In short, the [New York] statute's blanket grant of permission to eavesdrop [was] without adequate judicial supervision or protective procedures."[76]

[34] The *Berger* Court avoided the task of creating particularized guidelines and parameters that were applicable for a more in-depth Fourth

---

Surveillance Systems, 3 N.C. J. L. & TECH. 151, 169 (2001); *see generally* Mulligan, *supra* note 10.

[72] Berger v. New York, 388 U.S. 41 (1967).

[73] *Id.* at 49.

[74] *Id.* at 44.

[75] *See* Simmons, *supra* note 10, at 552 (2003)

> The Court held that orders issued under the statute would not conform to the particularity requirement, since the order need only describe 'the person or persons whose communications . . . are to be overheard.' . . . The Court [also] held that allowing the monitoring to continue for two months 'is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause.' . . . [And further, that] the Court was trouble by the fact that there was no mandatory termination of the order ... [or that there be a showing of] exigent circumstances in order to justify the lack of notice.

[76] Berger, 388 U.S. at 59.

Amendment analysis of electronic surveillance or its counterparts.[77] In recognizing this regulatory lag, the Court found, "[t]he law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge."[78] Similarly, in *Lopez v. United States*, the Court again recognized that "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual . . . . [I]ndiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments."[79] By failing to keep up with these types of advances, investigative methods utilizing these tools may continue to be carried out with little regulatory guidance.[80] Despite the Court's recognition that the law has not been able to keep up with technology, no default standard has been set.[81] Instead, issues involving video surveillance have been dealt with on a case-by-case basis on the federal appellate level, which has led to a jurisdictional rift in interpretation.

2. CLEAR SPLIT IN THE CIRCUIT COURTS

[35] In 1984, the Seventh Circuit became the first federal appellate court to consider and subsequently rule on surreptitious video surveillance as an investigative tool.[82] In *United States v. Torres*,[83] the Seventh Circuit

---

[77] *Id.*

[78] *Id.* at 49.

[79] Lopez v. United States, 373 U.S. 427, 441 (1963).

[80] Berger, 388 U.S. at 56 (Stewart, J., concurring). Justice Stewart's opinion in Berger underscores the need for heightened restrictions when dealing with an intrusive method of investigation, which in this case was trespassory eavesdropping through bugging devices. Justice Steward stated,

> The need for particularity and evidence of reliability in the showing required when judicial authorization is sought for the kind of electronic eavesdropping involved in this case is especially great. The standard of reasonableness embodied in the Fourth Amendment demands that the showing of justification match the degree of intrusion.

This analysis applies with equal force to covert video surveillance, though it was not at issue in Berger, as video surveillance has been characterized as more intrusive than the type of eavesdropping at issue here.

[81] Id. at 118 (White, J., dissenting). Justice White's opinion addresses the issue of whether "this case [is] a proper vehicle for resolving all of these broad constitutional and legislative issues raised by the problem of official use of wiretapping and eavesdropping." *Id*.

[82] Simmons, *supra* note 10, at 556-59.

emphasized the fact that no existing statute explicitly dealt with covert video surveillance, including both Title III and the Electronic Communications Privacy Act.[84] However, the court used Rule 41 of the Federal Rules of Criminal Procedure[85] to provide judicial authorization to grant warrants for such surveillance.[86] At first glance, this placed analysis of covert video surveillance under the ambit of general Fourth Amendment principles. Yet, the approach taken actually synthesized Fourth Amendment principles with some of the more narrow constraints applicable to other forms of electronic surveillance found in Title III.[87] Because Title III does not include video surveillance techniques but does address surreptitious aural interception, it was used as a guide in formulating the requirements for surreptitious visual interception. By interweaving these doctrines, the *Torres* court was able to impose more strict rules upon the use of video surveillance—a technique it found to be increasingly intrusive and in need of such additional constraints.[88]

[36] Following the *Torres* ruling, six other federal circuits joined the Seventh Circuit's reasoning and application of the standard used in *Torres* as the benchmark from which to begin interpretations of the

[83] United States v. Torres, 751 F.2d 875 (7th Cir. 1984) (reinforcing the notion that this particular issue had not yet been addressed).
[84] *Id.* at 877-82.
[85] FED. R. CRIM. P. 41(c) provides in pertinent part, Property or persons which may be seized with a warrant. A warrant may be issued under this rule to search for and seize any

> (1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense; or (4) person for whose arrest there is probable cause, or who is unlawfully restrained.

[86] *See* United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992) (stating that Rule 41(b) permits a district court to issue warrants for silent video surveillance); *see also,* United States v. Mesa-Rincon, 911 F.2d 1433, 1436 (10th Cir. 1990) ("Rule 41 is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause.") (quoting United States v. New York Tel. Co., 434 U.S. 159, 169 (1977)).
[87] 18 U.S.C. §§ 2510-2520 (2001).
[88] Simmons, *supra* note 10, at 558 ("[A] warrant for video surveillance should require a higher showing by the government than a warrant for a traditional search, and since video surveillance is 'identical in its indiscriminate character to wiretapping and bugging,' the rules which apply to wiretapping and bugging should also apply to video surveillance.").

constitutionality of surreptitious video surveillance. [89] The general standard implemented by these seven circuits, with slight departures, requires that a warrant based on probable cause must be properly issued by a neutral and detached judicial officer before such surveillance can proceed, just as required by the Fourth Amendment. By then looking to Title III's narrow requirements, these courts further require that for any investigation

> (1) the judge issuing the warrant must find that 'normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous . . . (2) the warrant must contain 'a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates,' . . . (3) the warrant must not allow the period of interception to be 'longer than is necessary to achieve the objective of the authorization . . . or in any event longer than thirty days,' (though extensions are possible) . . . and (4) the warrant must require that the interception 'be conducted in such a way as to minimize the interception of communications not otherwise subject to interception.'[90]

[37] While the remaining five circuits have adhered to the *Torres* court's characterization of video surveillance as an investigative technique that carries the potential for increased intrusiveness, they have not applied the Seventh Circuit's approach in their analyses. This divergence in judicial treatment has created a rift in the propriety of this investigative technique, leaving open the possibility for inconsistent evidentiary rulings from one jurisdiction to the next, irregularity in practices by police agencies, and confusion in understanding Fourth Amendment rights by defendants.

[89] The six circuits that have followed the Torres court's analysis include: Second Circuit in *United States v. Biasucci*, 786 F.2d 504 (2nd Cir. 1986); Third Circuit in *United States v. Williams*, 124 F.3d 411 (3rd Cir. 1997); Fifth Circuit in *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); Eighth Circuit in United States v. Falls, 34 F.3d 674 (8th Cir. 1994); Ninth Circuit in *United States v, Nerber*, 222 F.3d 597, 603 (9th Cir. 2000); and Tenth Circuit in *United States v. Mesa-Rincon*, 911 F.2d 1433, 1442 (10th Cir. 1990).
[90] Koyomejian, 970 F.2d at 542.

II. BYPASSING ANY JUDICIAL SCRUTINY: USE OF SNITCHES

[38] The confluence of the laws governing video surveillance and the use of undercover informants creates a doctrinal problem. Undercover informants - or snitches - are widely used today as a valuable and efficient investigative tool by police agencies.[91] The use of a consenting snitch in obtaining non-video surveillance has been recognized by the courts as unproblematic with regards to the Fourth Amendment.[92] Taking the analysis one step further, however, use of a consenting snitch to obtain surreptitious video surveillance effectively creates a regulatory loophole by allowing the investigating officers to bypass all procedural requirements upon obtaining the snitch's consent. By obtaining the consent of a snitch, the government is relieved of the procedural obligations as required by both the Fourth Amendment and Title III. It is in this scenario that the intrusiveness of video surveillance is essentially disregarded, since the protective mechanisms such as the warrant requirement and review processes no longer need to be satisfied.

A. CURRENT LAW GOVERNING THE USE OF SNITCHES IN UNDERCOVER INVESTIGATIONS

[39] The use of informants by law enforcement has become a widely utilized investigative mechanism. The basic "snitch" structure usually involves participating informants, who are commonly criminals themselves, agreeing to work alongside law enforcement officials in exchange for lenience or exculpation for past or present offenses.[93]

[40] Various scholars have commented on the legal and societal consequences that arise from this type of quid pro quo arrangement.[94] Common concerns include, but are not limited to: unjustified invasions of privacy, heightened intrusions on individual autonomy, entrapment, decreased social control, negative public perception of law enforcement

[91] *See* Susan S. Kuo, *Official Indiscretions: Considering Sex Bargains with Government Informants*, 38 U.C. DAVIS L. REV. 1643, 1649-50 (2005).
[92] *See e.g.*, Hoffa v. United States, 385 U.S. 293, 301-302 (1966).
[93] *See* Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. CIN. L. REV. 645, 651-52 (2004).
[94] *See generally id.*; *see also* MARX, *supra* note 12.

and the justice system, and instances of internal corruption.[95] These concerns have proliferated as the prevalence of undercover snitch investigations has rapidly increased.

[41] Judicial and legislative characterization of informant-aided investigations has lent support for this hybrid form of plea-bargaining benefiting the snitch, while bolstering arguments in favor of maintaining this practice in its current form.[96] Notwithstanding the greater ease and reliability associated with garnering evidence through snitch investigations, the practice of utilizing informants is left largely unregulated.[97]

[42] A line of cases decided by the United States Supreme Court and Title III of the Omnibus Crime Control and Safe Streets Act of 1968[98] illustrate favorable judicial and legislative treatment provided to snitch investigations. The current trend leans toward placing greater discretion at the hands of law enforcement, and less weight on the importance of the after-the-fact review process. The complacency by the courts with regards to use of snitches has led to confidence by law enforcement agencies in using confidential informants as a vehicle to carry out surreptitious video surveillance.

B. JUDICIAL INTERPRETATION OF THE USE OF SNITCHES

[43] The United States Supreme Court visited the topic of snitch investigations, in isolation, in a series of cases involving informants who, while acting in concert with the government, consented to surveillance of conversations that ultimately implicated their cohorts. The common thread in these decisions lies in the Court's finding that there is no reasonable expectation of privacy in conversations between criminal cohorts or co-conspirators regarding past, present, or future activities that are criminal in

[95] *See* MARX, *supra* note 12, at 33.
[96] *Id.* at 45-54 ("Recent judicial and legislative changes have encouraged the spread of undercover tactics in two general ways: indirectly, by creating new restrictions on conventional forms of police investigative behavior; and directly, by broadening their legal foundation." *Id*. at 46).
[97] Natapoff, supra note 93 at 669 (citing James Vorenberg, *Decent Restraint of Prosecutorial Power*, 94 HARV. L. REV.1521, 1566 (1981)).
[98] 18 U.S.C. §§ 2510-2520 (2001).

nature.[99] To add to this finding, the Court has also found that using technological tools (such as those used for electronic surveillance) adds no additional intrusion and no further violation of this privacy expectation.[100]

[44] In *On Lee v. United States,*[101] the Court validated the single-party consent rule, essentially finding that when one party to a conversation consents to the electronic surveillance of that conversation, there is no need to demonstrate probable cause or even to obtain a warrant, since those circumstances fail to implicate the Fourth Amendment or its requirements.[102] In *On Lee*, the government placed a microphone on its snitch, Chin Poy, which transmitted the contents of On Lee's incriminating statements to the agents located outside. The Court's analysis hinged on the fact that no physical trespass[103] had occurred since Chin Poy was considered an invited guest and found no violation of the surveillee's reasonable expectation of privacy.

[45] Similarly, in *United States v. White*, a tape-recorder placed on the person of an informant provided the Government with audiotapes containing incriminating statements made by the defendant which were admitted into evidence in lieu of the informant's testimony.[104] The Court re-characterized *On Lee's* single-party consent rule by focusing more heavily on the surveillee than on the snitch. The Court ultimately formulated its analysis on the theory of assumption of the risk rather than the affirmative consent of a cooperating snitch.[105] As one commentator

[99] *See e.g.*, Hofffa, 385 U.S. at 301-303.
[100] *See* Lopez v. United States, 373 U.S. 427 (1963).
[101] On Lee v. United States, 343 U.S. 747 (1952).
[102] *See* Captain Timothy A. Raezer, *Needed Weapons in the Army's War on Drugs: Electronic Surveillance and Informants*, 116 MIL. L. REV. 1, at 6 (1987).
[103] *Cf.* Katz v. United States, 389 U.S. 347, 351 (1967).
[104] United States v. White, 401 U.S. 745, 747 (1971).
[105] White, 401 U.S. at 751-52; s*ee*, Raezer, *supra*, note 102, at 15

> This theory [stated in *White*] was based upon the premise that the defendant did not have a reasonable expectation of privacy that the person with whom he spoke would keep the conversation secret. Because a party to a conversation can reveal it without violating the defendant's expectation of privacy, the consenting party's recording or transmitting of that conversation, likewise, does not violate the defendant's reasonable expectation of privacy. In short, a person assumes the risk that the other party to a conversation will reveal, transmit, or record it.

said, the Court found that, by talking to another person, the defendant surveillee had assumed the risk that his conversation would be repeated or was being recorded and consequently had no reasonable expectation of privacy in its contents.[106]

[46] The implications of *On Lee*'s ruling on more intrusive investigative techniques, such as covert video surveillance with snitches, are important to consider:

> Abolition of *On Lee* would not end electronic eavesdropping. It would prevent public officials from engaging in that practice unless they first had probable cause to suspect an individual of involvement in illegal activities and had tested their version of the facts before a detached judicial officer. The interest *On Lee* fails to protect is the expectation of the ordinary citizen, who has never engaged in illegal conduct in his life, that he may carry on his private discourse freely, openly, and spontaneously without measuring his every word against the connotations it might carry when instantaneously heard by others unknown to him and unfamiliar with his situation or analyzed in a cold, formal record played days, months, or years after the conversation. Interposition of a warrant requirement is designed not to shield 'wrongdoers,' but to secure a measure of privacy and a sense of personal security throughout our society.[107]

[47] While the general tenets of the assumption of the risk doctrine are meant to remove any benefit of the doubt criminal wrongdoers would retain in their illegal activities, the scope of this doctrine reaches much further. The majority of the Court has not visited this quandary, but Justice

[106] *Cf.*, Tom P. Conom, *Privacy and the Fourth Amendment in the Twenty-First Century*, 19 CHAMPION 13 (1995) The author criticizes the Court's decision in *White* by stating, "The Supreme Court adopted the false and pernicious assumption of the risk doctrine in which a citizen is said to forfeit all constitutional protections against electronic surveillance by the mere act of communicating with a fellow citizen." *Id*. at 13-14.
[107] White, 401 U.S. at 789-90.

Harlan visited the problem this carve-out creates in his dissenting opinion in *White*.[108]

> The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement. This question must, in my view, be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement. For those more extensive intrusions that significantly jeopardize the sense of security which is the paramount concern of Fourth Amendment liberties, I am of the view that more self-restraint by law enforcement officials is required and at the least warrants should be necessary.[109]

Despite this recognition, however, both Congress and the Supreme Court have left a hole in Fourth Amendment jurisprudence. By failing to recognize Fourth Amendment limitations when only one party to the conversation being surveilled has consented, the Court has created a path by which law enforcement officials can avoid the warrant requirement and its prerequisites.

[108] In *Lopez*, the Court ruled that the use of technological tools to heighten the reliability of evidence does not implicitly generate any greater intrusion than that which may be heard by the human ear, or recanted by the informant's memory. Lopez, 373 U.S. at 438. However, Justice Harlan made a point in *White* to clarify that this characterization, as found in both *Harlan* and *Lopez*, is not necessarily applicable to surreptitious video surveillance carried out in conjunction with informant consent. In his dissenting opinion he noted that "in *Hoffa*, Mr. Justice Stewart took care to mention that 'surreptitious' monitoring was not there before the Court, and so too in *Lopez.*" White, 401 U.S. at 758. Justice Harlan went on to further clarify that "the issue of the informer's consent to utilization of this technique is not properly before [the Court]." *Id*. at 771. *See also* Hoffa v. United States, 385 U.S. 293 (1966).

[109] White, 401 U.S. at 786-87 (Harlan, J. dissenting).

C. LEGISLATIVE INTERPRETATION OF THE USE OF SNITCHES

[48] Title III provides clear guidelines that make it lawful for a person "to intercept a wire, oral, or electronic communication,[110] where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[111] Essentially, Title III allows law enforcement to circumvent the warrant requirement, or any comparable prerequisite, if it utilizes a snitch in its investigation.[112] As long as a participating informant is a party to the conversation surveilled or recorded, the officers carrying out that investigation need not jump the numerous administrative hoops otherwise required.[113]

[49] In line with the Supreme Court's characterization, Title III's deregulation of snitch investigations is largely based on the doctrines of implied consent and assumption of the risk.[114] Assessing the convergence of Title III with the use of a snitch, Justice Harlan in his dissenting opinion in *United States v. White* found cause for concern:

> [T]he comprehensive provisions of Title III are evidence of the extent of congressional concern with the impact of electronic surveillance on the right to privacy. This concern is further manifested in the introductory section of the Senate Committee Report. Although §2511(2)(c) exempts

[110] Title III was amended in 1986 by the Electronic Communications Privacy Act (ECPA), which prompted the inclusion of "electronic communications" to wire and oral communications. 18 U.S.C. § 2701 (2000); *see also* S. REP. 99-541 (1986).
[111] 18 U.S.C. § 2511(2)(c) (2001).
[112] *See*, MARX, *supra* note 10, at 55 ("Most of the electronic surveillance associated with covert means is not subject to a warrant restriction because it occurs either in public or in situations where one of the parties consents… The single-party consent laws found in most states permit this.").
[113] *See*, Pub. L No. 90-351, 82 Stat. 197 (West 1968). The rationale for this relaxation of the Constitutional requirements can be gleaned from the legislative comments accompanying the statute.
[114] *See*, Slobogin, *supra* note 32, at 20-24. Despite an absence of exigent circumstances, some courts have sanctioned certain searches and seizures that have been conducted without a warrant. Rationales for permitting such warrantless action are based on the doctrines of implied consent and assumption of the risk. Namely, that an individual who engages in criminal conduct assumes the risk that their cohort is acting in concert with the Government, for the purpose of implicating that individual. This rationale goes hand-in-hand with the Supreme Court's adjudication of this issue.

> consensual and participant monitoring by law enforcement agents from the general prohibitions against surveillance without prior judicial authorization and makes the fruits admissible in court, see §2515, congressional *malaise* with such conduct is evidence by the contrastingly limited endorsement of consensual surveillance carried out by private individuals.[115]

[50] Nonetheless, the use of a snitch was recognized by the majority as a means to bypass the requirements of Title III.[116] As Harlan articulates, "All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant."[117] This sentiment is further aggravated by use of more intrusive means of surveillance such as video surveillance.

III. EXPLOITING THE REGULATORY LOOPHOLE: USING THE SNITCH TO OBTAIN SURREPTITIOUS VIDEO SURVEILLANCE

[51] The Supreme Court has not yet definitively ruled on the convergence of snitch consent and its impact on the regulation of covert video surveillance.[118] Current jurisprudence in this area is largely governed by the respective approaches taken by the lower circuit courts facing this dilemma. However, little or no consideration has been given by legislators or scholars as to the consequences of importing the single party consent doctrine or the assumption of the risk justification for the propriety of snitch-obtained evidence into the context of more intrusive video

[115] White, 401 U.S. at 791 (*italics in original*) (citing 82 Stat. 212, 18 U.S.C. §2510, S. REP. NO. 1097, at 69 (1968)).
[116] *See generally* White, 401 U.S. at 745.
[117] *Id.* at 788-89.
[118] *See* Conom, *supra*, note 106, at 20, n. 27

> The critical question is, does the Fourth Amendment apply to video surveillance so that video invasion of privacy may only be accomplished by prior judicial review and issuance of a limiting warrant? The federal courts of appeals which have to date considered this issue are unanimous that the Fourth Amendment *does* apply to video surveillance. However, the Supreme Court has not yet spoken.

surveillance gathering (as assessed by the courts to be issues of Title III and Fourth Amendment jurisprudence).[119]

[52] The most obvious ramification of this confluence of these distinct issues is its effect on the warrant requirement. Although Title III anticipates the use of snitches as a means of bypassing the default warrant requirement,[120] the statute fails to sanction video surveillance. Only through judicial application of Title III to investigations utilizing covert video surveillance, falling outside the explicit confines of the statute, are law enforcement officials provided the opportunity to bypass the warrant requirement[121] and maintain a heightened level of discretion in all aspects of the investigation. All that is needed is a cooperating informant—a snitch that consents to carrying out the surreptitious video surveillance. By projecting the one-party consent exception found in Title III as well as the assumption of the risk doctrine applied to more traditional methods of wiretapping, snitches make it easier for investigating officers to conduct their investigations without judicial or legislative scrutiny. Investigations can proceed without many of the common procedural requirements including but not limited to, prior judicial approval, [122] a foundational showing of probable cause particularity and limitations in the scope of the investigation, or ex post judicial review to ensure propriety of law enforcement actions. By advancing Title III into subject matter not contemplated by the legislature, the courts allow snitches to produce an investigatory carte blanche unregulated by the legislatures and unresolved by the courts.

[53] The application of assumption of the risk or single-party consent jurisprudence onto the incidence of snitch aided video surveillance is equally problematic. Directing this doctrine to a situation involving video

[119] Although the courts, legislators, and scholars have commented on the intrusiveness of video surveillance or on the use of snitches, generally, there has been no meaningful assessment of the implications of the convergence of the two areas.

[120] *See* Michael Goldsmith, *Criminal Law: The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance (Part 1 of 2)*, 74 J. CRIM. L. & CRIMINOLOGY 1, 3, n.1 ("Title III…does not cover so-called 'consensual' electronic surveillance in which one party…consents to the eavesdropping. 18 U.S.C. §§ 2511(c)-(d)").

[121] By bypassing the warrant requirement, I am referring to both ex ante authorization (including the showing of probable cause, particularity in the affidavit, and magisterial approval), as well as ex post review to ensure that the search was carried out properly.

[122] *See*, Slobogin *supra* note 32, at 107, n. 40.

surveillance is similarly inappropriate, without adequately taking the intrusiveness of this investigative method into consideration.

[54] With regards to both areas of jurisprudence, however, the regulatory inconsistencies and trivialization of the warrant requirement are the inevitable dangers of allowing this means of circumvention of the warrant requirement to stand in its current form.

A. REGULATORY INCONSISTENCIES ARISE FROM CIRCUMVENTION OF THE WARRANT REQUIREMENT

[55] By having neutral and detached judicial officers review and facilitate the execution of a traditional warrant, the grant of power and discretion is effectively bifurcated. Despite the fact that there are numerous other political entities that could take charge of regulating the scope and breadth of law enforcement activity, judicial officers act effectively in this role, as they are often the most impartial and detached party.[123] Since the law enforcement officials involved in the matter are purported to have a disproportionately greater interest in the outcome of the investigation, placing the grant of authority in the hands of judicial officers works to effectuate less bias within the judicial system by creating a system of checks and balances.[124]

[56] The interests at stake underscore the danger in irregularity of discretionary power. Because surreptitious video surveillance has the potential to thwart individual liberties and personal privacy interests more than other forms of traditional police searches and non-video surveillance, this regulatory inconsistency has far-reaching implications that have not even been considered. Professor Ric Simmons has commented on the regulatory inconsistencies in these types of hyper-intrusive searches, noting that, "The lack of a coherent constitutional framework for analyzing hyper-intrusive searches is all the more startling and problematic in an era when modern technologies and shifting political attitudes are generating new opportunities for the government to conduct ever more intrusive searches."[125] Furthermore, a blanket disposal of the warrant requirement

[123] *See*, *Id.* at 107.
[124] Natapoff, *supra* note 93 at 658.
[125] Simmons, *supra* note 10, at 549.

absolves the courts of the opportunity to articulate a stance on the use of more intrusive surveillance techniques by bootstrapping on the exceptions afforded to the use of snitches.

B. RENDERING THE WARRANT REQUIREMENT MEANINGLESS

[57] The assumption of the risk doctrine works to disintegrate any expectation of privacy a defendant may have, whether qualified by the circumstances or not. The ease with which this expectation is disregarded provides law enforcement with the opportunity to overstep their bounds, whether in fact justified or not. The rationales for stripping a criminal actor of his or her expectation of privacy when he or she is engaged in illegal activity have been stated by the Supreme Court.[126] However, the legitimacy of any generalized presumption, such as the assumption of the risk doctrine, must be questioned when it is indiscriminately extended to particularized circumstances such as the use of new surveillance technologies.

[58] If the assumption of the risk doctrine extinguishes any existing expectation of privacy one might have when they are dealing with criminal cohorts, shouldn't one first be aware that such a risk is present if they are held to have assumed it? "In order to assume a risk, one must first *know* what the risk is."[127] Tom P. Conom visits the counterintuitive foundation of the assumption of the risk doctrine, as set forth in *White*, by noting:

> Unless the *White* plurality truly is willing to saddle American society with the universal risk that every conversation may be electronically monitored, then the *White* plurality view is not only illogical and unreasonable—it is absurd. Moreover, it defies common sense as well as the common understanding of Americans who yet have some sensitivity to the 'qualitative difference' between electronic surveillance and conventional police investigation.[128]

[126] *See generally* United States v. White, 401 U.S. 745, 747 (1971); s*ee also* Hoffa v. United States, 385 U.S. 293, 293(1966).
[127] Conom, *supra* note 106, at 18.
[128] *Id.*

If a snitch is wired with a hidden video camera which captures incriminating evidence beyond the scope of the snitch's conversation with the surveillee, it should be unreasonable to presume that the surveillee assumed such a risk by merely conversing with a cooperating informant.

[59] Professor A. Westin has observed the societal consequences that may develop as long as snitch consent continues to provide this regulatory loophole in the context of the expanding area of hyper-intrusive searches:

> Allowing eavesdropping with the consent of one party would destroy the statutory plan of limiting the offenses for which eavesdropping by device can be used and insisting on a court-order process. And as technology enables every man to carry his micro-miniaturized recorder everywhere he goes and allows every room to be monitored surreptitiously by built-in equipment, permitting eavesdropping with the consent of one part would be to sanction a means of reproducing conversation that could choke off much vital social exchange.[129]

If this were the case, societal distrust and inter-social withdrawal would permeate American culture, even among those not involved in illegal or criminal activities. In addition to this "denigration of [the] individual is the damage undercover police work causes to the democratic state's objective of remaining legitimate. First, because it relies on fraud and deceit, covert investigation undermines trust in the government. More important, it increases distrust in *everyone*, since anyone could be a government agent."[130] Every individual would perpetually be walking on eggshells for fear that any misstep—even in the presence of close friends or family—could be used against them, regardless of any perceptual privacy interest they may hold. This is not the type of societal interaction America should be looking forward to.

[60] Cooperating snitches that consent to such monitoring are not held to the same standard of accountability, but rather, are allowed to engage in otherwise illegal conduct under the administrative shield against

[129] White, 401 U.S. at 789, n.23.
[130] Slobogin, *supra* note 32, at 104.

liability.[131] Ultimately, these snitches have become the tools by which law enforcement officials and investigators have been able to violate otherwise viable privacy interests without repercussion or suppression. Supreme Court decisions, which allow undercover police activity to proceed without ex ante execution of a valid warrant trivializes individual rights and interests by garbling the underlying basis for the assumption of the risk doctrine.[132] A snitch's unilateral consent, in and of itself, should not be deemed an automatic grant of blanket authorization to engage in any method of investigation without regulation, guidelines, or parameters. Yet the current state of jurisprudence in this area grants this very sort of boundless sanction,[133] thereby rendering the protections of the warrant requirements ineffective and the process of obtaining a warrant meaningless.

C. INEVITABLE ABUSES BY LAW ENFORCEMENT OFFICIALS

[61] The confluence of the regulations governing both snitch consent and video surveillance currently allow (and even endorse) law enforcement officials to make an end-run around the very constitutional safeguards set in place to limit the scope of their authority. Several cases decided by the Supreme Court[134] have accentuated the notion that law enforcement discretion must be limited, as they are not suited to place limits on their own authority.[135]

[62] In *Johnson v. United States*,[136] the Supreme Court went great lengths to underscore the importance of the warrant requirement in the preservation of individual rights against the threat of excessive police discretion.

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law

[131] *See generally* Natapoff, *supra* note 93.
[132] *See* Slobogin, *supra* note 32, at 107.
[133] Id.
[134] *See e.g.* Katz v. United States, 389 U.S. 347, (1967); Beck v. Ohio, 379 U.S. 89, 96 (1964); Johnson v. United States, 333 U.S. 10, 13-14 (1948).
[135] *See* Slobogin, *supra* note 32, at 29 ("In light of the police's tendency to be overly suspicious and to undervalue individual prerogatives, we might want to force them to seek authorization in every case.").
[136] Johanson, 333 U.S. 10 (1948).

> enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers…The right of officers to thrust themselves into a home is also a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of a search is, as a rule, to be decided by a judicial officer, not by a policeman or a government enforcement agent.[137]

Snitch consent, by eliminating the need for a warrant, has denigrated this principle of power-shifting and has worked to promote the very situation the Supreme Court in *Johnson* so vehemently condemned.

[63] The Court in *Beck v. Ohio* also criticized these law enforcement principles when it noted that the investigators' failure to obtain a warrant in *Katz* substituted "the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment."[138]

[64] Placing this almost immeasurable amount of discretion in the hands of law enforcement officials provides them the opportunity to engage in surveillance (searches and seizures) in an indiscriminate manner with the opportunity to fill in the gaps of minimization, necessity, and particularity after-the-fact. This discretion permits police officers to invade otherwise protected rights with minimal fears of penalization by means of ex post review, suppression, or reprimand.

[137] *Id.* at 13-14.
[138] Beck, 379 U.S. at 96.

[65] The consequence of this regulatory loophole is the increase in the potential for abuse. We already face an inherent dilemma in our current method of dealing with exploitation of police discretion. The efficacy of the exclusionary rule as a deterrent for the abuse of police authority has consistently been questioned.[139] Permitting blanket discretion on more violative intrusions, by means of circumvention of the warrant requirement, will further confound attempts at discouraging unlawful police action and unjustified personal intrusions.[140] Ignoring this gap in regulation has the potential to allow, or even promote, reprehensible police conduct that may go unpunished. Insofar as this heightened level of discretion is provided, abuses of law enforcement authority may continue to run rampant, without fear of regulatory intervention. As police power escalates, so may societal distrust and antipathy.

IV. CONCLUSION

[66] In the current world of digital technology where innovations and advancements are progressing by the millisecond, video cameras, video surveillance, and visual recording equipment are now considered obsolete technology. Without regulation of technology that has been widely used by the general public for several decades, what can we expect of regulations for up-and-coming advances in tools that can intrude on an individual's personal privacy?

[67] By continuing on a regulatory path lacking specifically tailored legislation, particularly in dealing with the troublesome combination of snitch cooperation and covert video surveillance, we are perpetuating a problem that will only inflate at the rate of technological innovation.

[139] *See generally* Slobogin, *supra* note 32, at 8-12 (arguing that the United State's exclusionary rule, which is meant to act as a deterrent against unlawful police behavior, is ineffective as there is not direct penalization that effects the law enforcement officer—rather, it is the suppression of evidence that acts as a slap on the wrist).

[140] *See Id.* at 36-37. Police discretion is not minimized significantly by administrative or regulatory procedures, which attempt to create some sort of standardization in dealing with this matter. There still needs to be some kind of ex post review system to ensure that law enforcement officials are always held responsible to answer to an authority, to report on their actions and conduct, and to conduct themselves with the foresight of possible reprimand for improper behavior or actions.

Advances in technology, such as facial recognition technology[141] and biometrics, will only provide law enforcement with future surveillance equipment and unimaginable tools that invade the most intimate of locations.[142]

[68] Even at this point, however, Fourth Amendment jurisprudence has not ventured into the present circumstances, let alone future horizons, while allowing regulatory loopholes to suppress judicial and legislative grappling of the important issues. Without a strong resolve to establish a uniform framework of the protections of the Fourth Amendment and a resolve to refrain from expounding on old frameworks while overlooking important advancements and distinctions, a slippery slope will render our Fourth Amendment rights and protections a fiction.

[141] *See generally*, Milligan, supra, note 14 at 309-11 (showing how investigators can match a face to a specific name or an image and retrieve tremendous amounts of information on that individual including information, the existence of which, is unknown to the subject).

[142] *See generally* Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. TECH. L & POL'Y 143 (2004).