In God We Trust; All Others Who Enter This Store Are Subject to Surveillance(1)

Karen A. Springer(1)

Introduction

Until May 1994, Americans had reason to believe that doughnut shops were bastions of friendliness and safety. Where else, after all, can one enjoy both a cup of coffee and the security of police officers at virtually any hour? Then, over Memorial Day weekend, the illusion was shattered when a story broke: At some East Coast Dunkin' Donuts, the "walls have ears(1)—in the form of hidden microphones that record not only customer purchases but their private conversations as well.(2)

Used by some Dunkin' Donuts to prevent theft and monitor customer service at the point of sale, the surveillance equipment could pick up conversations from a distance of thirty feet.(3) This news surprised customers in two microphone-equipped Dunkin' Donuts in Concord, New Hampshire. "It sounds like Nazism or the KGB. It's not American," said Nick Hondrogen. "Many times you say things to close friends you don't want overheard.(4)

But caveat emptor: Businesses might be eavesdropping on customers as they speak. No longer content with the commonplace surveillance cameras and anti-shoplifting mirrors, store owners have resorted to surreptitious audio monitoring of their employees and customers.(5) Concealed microphones lurk in department store clothing racks, super- markets, retail and convenience stores, and fast-food restaurants.(6) Yet, until the surveillance practices of Dunkin' Donuts were exposed, even consumer-privacy advocates knew little about such practices.(7) Despite the onslaught of negative publicity, audio surveillance will continue, warns one electronics company executive.(8) "[U]ntil . . . there is minimal crime in this country, . . . store owners are going to have these devices to protect their employees and their customers," said Lewis Weiss, Chief Executive Officer of Louroe Electronics of Van Nuys, California.(9)

Indeed, the trend is not toward pulling the plug on hidden bugs.(10) One report analyzing private-sector markets for security surveillance and monitoring equipment predicted a $4 billion industry by 1998.(11) That represents an 8.6 percent annual increase in the demand for sophisticated equipment that includes closed-circuit television (CCTV) and listening devices.(12) According to the publisher of the report, one of the best opportunities for equipment sales lies in the business-services sector due to its high losses.(13)

If businesses continue to engage in surreptitious audio surveillance,(14) however, they risk combatting crime with crime. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)(15) establishes national standards to regulate the use of electronic surveillance, and those standards are to be strictly construed.(16) Title III sets forth baseline requirements, and individual states may enact their own equally or more stringent laws.(17) As of 1991, all but four states prohibit, except under specific circumstances, the interception of oral, wire, and electronic communications by both law enforcement and the private sector.(18) The state of New Hampshire, where the Dunkin' Donuts surveillance was uncovered, has a wiretap statute even more restrictive than Title III.(19)

While the security measures employed at Dunkin' Donuts may be common in businesses that suffer high cash and product losses, their use in what should be speech-friendly establishments strikes as egregious conduct. Ron Tudor, an agent with the Florida Department of Law Enforcement, said it best when he described his reaction to the audio surveillance at Dunkin' Donuts: "I have what I consider a reasonable expectation of privacy when I sit down in the booth of a restaurant. I shouldn't have to worry about someone listening in on my conversa tion.(20)

Using the Dunkin' Donuts setting for purposes of analysis, this Note examines the standards established by Title III. Part I of this Note provides specifics as to the audio surveillance used by Dunkin' Donuts. Part II offers a brief overview of the latest failed attempt to regulate surveillance in the workplace. Part III presents the legislative history of Title III. Part IV applies the operative statutory language to the Dunkin' Donuts scenario. Part V examines problems with the enforcement of Title III. This Note concludes that, as a consumer, Ron Tudor should not have to worry about businesses furtively recording his personal conversations, but he may have little choice. The insidious nature of

bugging makes violations of Title III difficult to detect. Further, even if detected, those violations may offer little in the way of adverse consequences to violators. As a result, bugs continue to multiply. Short of carrying a "countersurveillance probe/monitor" to detect lurking bugs,(21) consumers enter our nation's stores armed with little more than ineffective statutory prohibitions to combat the creeping phenomenon of private-sector bugging.

I.Audio Surveillance Arrives at Five Dunkin' Donuts

Around October 1993, five Dunkin' Donut franchises in New Hampshire contracted with an in-state security firm for the purchase and installation of surveillance equipment as part of their ongoing loss- prevention measures.(22) The equipment consisted of four cameras and one microphone having the capacity, according to those who purchased it, "to produce [an] audio recording of employees' conversations and, in some instances, of customers" in each store.(23) The two officers and/or directors of the franchises claim to have purchased the equipment upon their belief that audio recording was legal in New Hampshire.(24)

As of May 27, 1994, each franchise had approximately twenty-one tapes in use.(25) What was recorded on those tapes depended upon camera locations, the level of background noise, and the volume of the speakers' voices.(26) Although the franchise representatives denied intending to record their customers' conversations, they did not deny having in fact done so.(27) The audio surveillance continued for approximately six months until a curious customer inquired about the operation of the video cameras.(28) That customer—who was merely looking to buy a cup of coffee and a Boston "kreme" doughnut—happened to be an investigator for New Hampshire's Consumer Protection and Antitrust Bureau.(29) He found a surveillance system that "pretty clearly picked up" the conversations of customers in areas far removed from the checkout counter.(30) In addition to a master audio pickup located near the cash register, each of the four mounted cameras had standard audio components and the ability to pan the entire shop.(31)

II.A Failed Attempt to Regulate Workplace Surveillance

While this Note does not focus upon the evils of employee surveil lance in the workplace, practices directed at employees obviously affect customers. Unfortunately, while Congress makes repeated attempts to regulate workplace surveillance,(32) it remains indifferent to the plight of consumers.

The latest unsuccessful attempt to regulate workplace surveillance appeared as House Bill 1900(33) and Senate Bill 984,(34) the Privacy for Consumers and Workers Act. Despite its name, the Act had little to do with protecting consumer privacy. The content of the bills—and their ultimate defeat—demonstrates the lobbying power behind retail, security, and restaurant interests. These very interests, of course, promote and use covert electronic surveillance as a loss-prevention measure. As a result, they represent a significant threat to privacy for consumers and the remedial effects of Title III.

The Privacy for Consumers and Workers Act received vehement criticism for overbreadth by retail(35) and security lobbyists.(36) Further criticism caused Representative Pat Williams (D-Mont.) to modify House Bill 1900 "to accommodate the reasonable concerns" voiced by the National Restaurant Association and the National Association of Conve nience Stores.(37) However, even in its original form, the Act virtually endorsed the covert audio surveillance utilized by Dunkin' Donuts. As introduced, Section 9 of the bill regarding privacy protections provided:

(2) EXCEPTION.—Electronic monitoring by an employer whose purpose and principal effect is to collect data about the work of an employee *or to collect data on subjects who are not employees of the employer* is not prohibited . . . because it incidentally collects data which is not confined to such employee's work.(38)

Further, the public-notice requirement contained in House Bill 1900 acknowledges both the lack of a surveillance prohibition upon employers and the resultant encroachment on customer conversations. Recognizing the spillover, the requirement provided for notice reasonably calculated to reach members of the public included in or affected by the employer's electronic monitoring.(39) This notice requirement serves as the only acknowledgment in House Bill 1900 of any kind of consumer privacy interest.

Security professionals discounted even that small interest as they insisted that privacy take a back seat to safety. In its September 1993 position statement to Congress, the American Society for Industrial Security (ASIS) said that "[t]he

nation's security professionals feel that the debate over electronic monitoring should center on the public's safety and security rather than on potential, and in some cases illusory, privacy abuses that can be adequately addressed by existing federal and state laws.(40)

Clearly, the interests that utilize and promote covert audio surveillance use their considerable power to maintain the bugging status quo. Consumers must look over their shoulders—and backward in time—for protection from furtive bugs. To evaluate the protection afforded by existing federal law, we turn to Title III.

III.A Legislative History of Title III

A. Underlying Goals of Title III

Despite legitimate law enforcement needs, rapid technological advances in the 1960s created the opportunity for "widespread use and abuse of electronic surveillance techniques" to combat organized crime.(41) In 1968, the Senate Committee on the Judiciary identified the problem as follows: "Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advan tage.(42)

To remedy this "intolerable" situation,(43) Congress enacted Title III to accommodate both law enforcement and privacy interests. Title III has the dual purpose of protecting the privacy of oral and wire communications and delineating a uniform standard for authorizing the interception of those communications(44) in efforts against crime.(45) The Act sought to conform electronic surveillance practices to the constitutional standards established by the United States Supreme Court in two cases: *Berger v. New York(46)* and *Katz v. United States*.(47)

B. Why Title III Applies to Dunkin' Donuts

While Title III primarily targeted the problems connected with organized crime and unauthorized surveillance by the government, Senate Report 1097 clearly establishes that the Act extends to electronic surveil lance conducted by the private sector. "To assure the privacy of oral and wire communications, *[T]itle III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers. . . .*(48) There are three exceptions to this blanket prohibition. Business is not one of them, and the omission was intentional.

In 1965, the Subcommittee on Administrative Practice & Procedure of the Senate Judiciary Committee held hearings on the necessity of legislation to protect individual privacy from nongovernmental surveillance. It identified three areas of widespread electronic surveillance by nongovern mental actors. Subcommittee Chairman Long offered the following insight: "The three large areas of snooping in this [nongovernmental] field are (1) industrial, (2) divorce cases, and (3) politics. So far, we have heard no real justification for continuance of snooping in these three areas.(49) More over, Senate Report 1097 indicates that interceptions "by private unautho rized hands have little justification(50) without the consent of one party to the targeted communication. The unambiguous language of Title III itself reflects this belief. Therefore, Title III applies to operations such as Dunkin' Donuts.

C. What Title III Prohibits

Except as specifically provided, Title III proscribes the actual or attempted intentional interception of wire, oral, and electronic communica tions as well as the disclosure or use of any communication intercepted.(51) For any unlawful interception, Title III prescribes criminal penalties of not more than five years imprisonment, a fine, or both;(52) civil recourse for actual or statutory damages sustained;(53) and the suppression of evidence obtained.(54) Title III further proscribes (with limited exception) the intentional manufacture, possession, mailing, or advertisement of electronic, mechanical, or other devices known to be used primarily for the surreptitious interception of oral, wire, or electronic communications.(55)

Title III does not proscribe interceptions made with consent, regardless of whether those acting under color of law or private individuals make the interceptions.(56) A consensual interception by law enforcement occurs when the government actor is a party to the intercepted communica tion or when a party to that communication gives prior consent.(57) A consensual interception by a private actor occurs in the same way; however, interceptions made for the purpose of committing a criminal or tortious act are prohibited.(58) Accordingly, Title III prohibits Dunkin' Donuts from making nonconsensual interceptions and consensual intercep tions that have a criminal or tortious purpose.

D. Those Exempt from the Prohibition

Under Title III, law enforcement personnel conducting an investiga tion of certain major crimes can perform wiretaps and other electronic surveillance when they have obtained court authorization upon a showing of probable cause.(59) While engaged in the ordinary course of their business, employees of communications providers(60) and the Federal Communications Commission (FCC)(61) are also exempt from the prohibi tions of Title III. Further exempted are government officials acting under presidential power to protect national security interests.(62)

IV.Analysis of Title III

A. When Does a Private Conversation Qualify as an Oral Communication?

To determine whether a Title III violation has occurred, one must first consider the nature of the intercepted communication. For Title III purposes, an "`oral communication' is a term of art.(63) The import of the term lies in the communicator's expectations and not in the communi cation's oral nature.(64) A conversation qualifies as an oral communication when it is "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication . . . .(65) Pursuant to these requirements, a conversation held in an establishment such as Dunkin' Donuts would generally constitute an "oral communication." Aside from the obvious circularity of defining the term "oral communication" with the term itself,(66) the operative language of Section 2510(2) is a two-prong test that consists of a subjective and an objective expectation. The test evolved from the Supreme Court's landmark decision in *Katz*,(67) which involved Fourth Amendment protections, and particularly from Justice Harlan's concurring opinion. "[T]here is a twofold requirement," Harlan stated. "[F]irst, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as `reasonable.'(68) The subjective expectation thus represents a question of fact, while the objective expectation represents a question of law.(69)

1. The Subjective Expectation

The first element of the subjective requirement—any oral communica tion(70)—is satisfied as long as the parties communicate with spoken words. To satisfy the second element of the subjective requirement, the conver sants must exhibit an actual expectation that their communication will not be intercepted.(71) If the parties have no reason to believe that Dunkin' Donuts utilized audio surveillance, it follows that they would have an expectation that their exchange was private. Unless they conversed in a loud or otherwise distracting manner, they would also exhibit an expecta tion that their conversation would not be overheard by others nearby.

Conversation over coffee and doughnuts might well include the intimate details of people's lives. If the speakers take care not to be overheard by persons within sight and earshot, they surely do not expect their conversation to be intercepted by a hidden electronic eavesdropper, regardless of its proximity. The very nature of the conversation would confirm the assumption of a private exchange. On this basis, the subjective prong of the "oral communication" test is met under the Dunkin' Donuts analysis.

2. The Objective Expectation

The objective prong of the "oral communication" test presents a greater hurdle under Title III, both to civil plaintiffs

seeking monetary damages and to criminal defendants seeking Fourth Amendment protection. This hurdle often proves impossible to overcome because under its *Katz* analysis, the Supreme Court takes an extremely narrow view of what constitutes reasonable privacy expectations.

a. The Unambiguous Language of Section 2510(2)

Of what concern, one might legitimately ask, are objective expecta tions of privacy to a Title III analysis? The unambiguous language of Section 2510(2) requires an expectation that the communication "is not subject to *interception*. . . .(72) Standard rules of statutory construction command that absent a clear legislative intent to the contrary, unambiguous language "must ordinarily be regarded as conclusive.(73) Nor can it be ignored that Congress defined what it meant by an interception. "`[I]nter cept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.(74) A court cannot, like Humpty-Dumpty, interpret the plain language of Section 2510(2) to mean something different than what it says.(75) The appropriate objective test under Title III, therefore, does not involve reasonable expectations of privacy. Rather, it involves reasonable expectations of noninterception, which is not a semantic distinction without a difference.

First, an expectation of noninterception imposes a different, and arguably lesser, burden upon the party whose conversation has been intercepted. The Eleventh Circuit acknowledged this tension but was not required to resolve it in the case of *Walker v. Darby*.(76) The Eleventh Circuit expressly distinguished expectations of noninterception from those of privacy in a civil suit brought by a postal employee against his supervisor. Sympathetic to Walker's complaints that his employer bugged his work station, the court said: "[W]hile Walker might have expected conversations uttered in a normal tone of voice to be overheard by those standing nearby, it is highly unlikely that he would have expected his conversations to be electronically intercepted and monitored in an office in another part of the building.(77)

However, the Eleventh Circuit did not reach this issue of objective expectations of noninterception. It reversed the post office's grant of summary judgment and remanded for further proceedings for a factual determination as to Walker's subjective expectation.(78) Even though the court's analysis is dicta, the point is well taken that reasonable expectations of privacy are more limited than are reasonable expectations of noninter ception. Because the concepts are not identical, a person may lack the former but still have the latter.(79)

Second, an expectation of noninterception directs the focus away from generalizations about the public nature of the locality to a specific consideration of its function. While jails, for example, are not "open to the public," the courts have held there is no reasonable expectation of privacy in them.(80) However, the crowded and communal conditions of our jails do not make expectations of privacy and noninterception within them unreasonable. Rather, because the sole purpose of a jail is to confine known or suspected criminals, it is reasonable to expect that others will intercept communications(81) and monitor behavior in order to protect both inmates and their keepers. Thus, if certain types of facilities lend themselves to the inflexible determination that an expectation of noninter ception will never be justified within them, the function and not the form of the facility is determinative. As for jails, that determination also flows from the legislative history of Title III, which declares that no expectation of privacy exists therein.(82) Accordingly, appellate and state courts have resolved this question of law against both criminal defendants(83) and civil plaintiffs.(84)

While Dunkin' Donuts is not a jail, neither legislative history nor judicial precedent tidily resolves whether customers have an expectation of noninterception in such an establishment. However, it does not stretch the logic of either legislative history or judicial precedent to suggest that the very function of a Dunkin' Donuts or similar operation supports an expectation of noninterception.

When customers chat and linger over coffee, they do so at the express invitation of Dunkin' Donuts, which installs booths and tables for their dining convenience(85) and creates an atmosphere conducive to conversa tion. Accepting that invitation, customers spend more than one billion dollars annually at Dunkin' Donuts.(86) As hoped for by Dunkin' Donuts, customers respond to sixty million dollars worth of advertising(87) launched to promote a "mainstream premium product available for the mainstream of America.(88) In return for its patronage, that mainstream received the shocking news that bugs had infiltrated Dunkin' Donuts. "[It is] the kind of thing that many of us got used to if we

traveled behind the Iron Curtain, when there was an Iron Curtain," said Laurence Tribe, professor of constitutional law at Harvard.(89) It is not, however, the kind of thing that many of us would expect at home, particularly in an eatery that promotes its fare and a comfortable environment in which to enjoy it. Clearly, the very function of a Dunkin' Donuts affords its customers a reasonable expectation of noninterception.

b. *Katz* Reasonable Expectations of Privacy: Has There Been a Knowing Exposure?

While noninterception analysis comports with the actual language of Section 2510(2), that, unfortunately, is not the interpretation given to it by the courts. Instead, courts think in terms of reasonable expectations of privacy afforded by the Fourth Amendment.(90) Of course, because the Dunkin' Donuts interceptors are private as opposed to government actors, Fourth Amendment protections are not implicated. Still, Title III was modeled upon the constitutional standards established in *Katz(91)* that: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.(92) Thus, the inquiry becomes whether Dunkin' Donuts customers who converse as they eat have knowingly and sufficiently exposed statements to outsiders so as to render those communications subject to interception and hence not "oral communications" within the meaning of the statute.

Following Justice Harlan's *Katz* concurrence, courts have generally found that "conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.(93) For example, the Seventh Circuit in *In re John Doe Trader Number One* held that a trader on the floor of the Chicago Mercantile Exchange had no reasonable expectation of privacy in the statements he made to an undercover FBI agent wearing a concealed tape recorder.(94) The court found Doe to have assumed the risk that his statements would be overheard and recorded.(95) There is, however, nothing remarkable about the court's reasoning or its conclusion. The agent who recorded Doe's remarks was either a participant to the conversations or stood within earshot of them. Because the agent was wearing the concealed recorder, it followed him and essentially "heard" the same things the agent heard.

The Dunkin' Donuts fact pattern is distinguishable from *In re John Doe Trader Number One*, however, and the differences are key to the analysis. The Dunkin' Donuts interceptor is not a participant in the conversation; the interception is similar to one made by a third person who is not within the earshot or eyesight of the conversants. As a result, the normal precautions used to guard against being overheard are not available to Dunkin' Donuts customers.(96) For this reason, they simply cannot be said to have assumed the risk, as did Doe, that their conversations would be overheard and, thus, able to be recorded. This distinction alone places a conversation held in a Dunkin' Donuts squarely outside the *In re John Doe Trader Number One* rationale and within the realm of concerns voiced by Justice Harlan nearly twenty-five years ago: "[I]t is one thing to subject the average citizen to the risk that participants in a conversation with him will subsequently divulge its contents to another, but quite a different matter to foist upon him the risk that unknown third parties may be simultaneously listening in.(97)

The emphasis in *In re John Doe Trader Number One* that either participant to a conversation is free to later relay its contents misses the mark in the case of Dunkin' Donuts: It fails to address the nature of third- party interceptions. Blackstone long ago said that, "eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance.(98) Moreover, Justice Holmes condemned the practice as "such dirty business.(99) When Justice Harlan distinguished between third-party and participant interceptions in *United States v. White*,(100) he recognized a crucial factor that the plurality appeared to overlook: A greater invasion of privacy occurs when the contents of an oral communica tion have been intercepted by a nonparty than if one of the participants later repeats any portion of that conversation.(101)

Further compounding the injury of third-party interceptions is the increased possibility of negative results. Communication would be inhibited, Justice Harlan contended, if one's conversations were thought to be at risk of full recording and accurate transcription.(102) This logic squares with the rules of evidence governing the inadmissibility, with certain exceptions, of hearsay testimony at trial: Error and oversight are inherent in the way humans report and especially repeat information. Cold reliability, on the other hand, is the threat represented by the recording and ultimate verbatim reporting of a conversation. Such a threat can effectively chill communications when speakers understand that their every word may be repeated verbatim—both to persons and by persons in whom they did not intend to

confide. Justice Harlan addressed this concern when he said: "Were third-party bugging a prevalent practice, it might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life.(103)

Certainly, an innocent conversation between friends, family members, or business associates who linger over coffee in a Dunkin' Donuts falls squarely within the categories of discourse that Justice Harlan sought to protect. And just as certainly, informal conversation between intimates often contains agreeable falsehoods, exaggerations, obscenities, and even antisocial views that the speaker does not expect to be taken seriously.(104) Yet, a greater disclosure than was intended can serve not only to embarrass the speaker but may lead to adverse consequences such as the loss of respect, or a job, or friends.(105) The threat thus represented by third-party interception can only inhibit the communications upon which personal relationships depend.(106) Such a result is neither intended by Title III nor desirable as a matter of social policy.

c.*Katz* Reasonable Expectations of Privacy: "What has Technology Wrought?(107)

Another issue related to the *Katz* reasonable-expectation-of-privacy analysis is the extent to which it has been influenced by technological advances in surveillance techniques.(108) In the Fourth Amendment criminal context, the United States Supreme Court has demonstrated a considerable tolerance for electronic intrusions and a concomitant intolerance for what individuals therefore "knowingly expose" to the public.(109) As a result, an individual's "`knowing exposure' may be entirely inadvertent or the result of continuing advances and applications of new surveillance . . . techno- logies.(110) Thus, criminal defendants have been found to have no reason able expectations of privacy against governmental intrusion in the telephone numbers they dial;(111) in opaque, closed garbage bags left on a residential sidewalk for collection;(112) or in a backyard marijuana crop concealed by a fence that could not be seen through or over.(113)

Of course, these cases differ from Dunkin' Donuts because they involve Fourth Amendment protections for criminal defendants and electronic surveillance other than eavesdropping. However, it does not advance the analysis to consider different standards of reasonableness for criminal and civil complainants. First, the suggestion that the laws should accord lesser privacy expectations to those who engage in criminal behavior ignores a powerful argument that criminal defendants should receive greater leeway to balance the force of governmental power brought to bear upon them. However, it is troublesome to suggest that civil plaintiffs, being innocent of criminal wrongdoing, should not have their legitimate expectations of privacy recognized. Second, and more important, the criminal/civil distinction does not affect the outcome because the United States Supreme Court has afforded civil plaintiffs the same constricted expectations of privacy as criminal defendants.

In *Dow Chemical Co. v. United States*,(114) the Supreme Court denied Dow any Fourth Amendment protection from Environmental Protection Agency (EPA) aerial surveillance and telephotography of land adjacent to a company plant. Consistent with its members-of-the-general-public rationale utilized in criminal cases, the Court concluded that the EPA's $22,000 aerial mapping camera was not "some unique sensory device that, for example, could penetrate the walls of buildings and record conversa tions in Dow's plants, offices, or laboratories, but rather a conventional, albeit precise, commercial camera commonly used in mapmaking.(115) Thus, the Court's understanding of "reasonable expectations of privacy" does not depend upon the civil or criminal nature of the proceeding. Rather, it appears to depend upon whether the general public could lawfully discover, with the aid of "non-unique" sensory devices, that which another seeks to protect as private.(116) In effect, the Court ignores whether a given technology "places individuals at risk of involuntary exposure that exceeds generally acceptable social norms.(117) The Court also relieves the interceptor from demonstrating both its need for and benefit from the invasive practice.(118)

If this members-of-the-general-public analysis were applied to Dunkin' Donuts, however, the pendulum would swing in favor of the intercepted party. That is because while the law does not prohibit the general public from flying at FAA-approved altitudes and observing whatever lies below, it does prohibit the general public from intercepting oral communications without prior consent.(119) Accordingly, Dunkin' Donuts customers do not "knowingly expose" the contents of their conversations to the public under *Katz*.(120)

d. Reasonable Expectations of Privacy: Do They Exist in Fitting Rooms?

Fitting-room cases stand for two propositions of particular appli- cability to the Dunkin' Donuts Title III analysis. As it pertains to the objective prong of the "oral communication" test, a customer's reasonable expectation of privacy in a business establishment depends upon common habits in the use of the property as well as upon the particular circumstances.(121) In both criminal prosecutions of a customer and civil actions against a retailer, the reasonable-expectation-of-privacy analysis focuses on the propriety of the fitting-room surveillance and not its results. Propriety and the reasonableness of the customer's expectation are questions of fact that require inquiry into the particular circumstances and the obvious conditions of the room.

Thus, in *In re Deborah C.*,(122) the California Supreme Court held that a juvenile shoplifter had no reasonable expectation of privacy in a fitting room where two-foot gaps above and below the door allowed for her activities to be observed by a store detective who stood in a normal position in the corridor.(123) Citing the configuration of the fitting-room door, the court reasoned that "[t]hough designed perhaps to give minimal protection to modesty, the doors hardly could promote any reasonable feeling that all actions and objects behind them were insulated from public observation.(124)

Dunkin' Donuts customers, however, do not seek to insulate themselves from public observation by persons who have a right to be where they are. Neither do those customers seek Title III protection from being overheard by persons who have assumed normal positions nearby. Rather, Dunkin' Donuts customers seek insulation from hidden micro phones that intercept their private conversations. As one fitting-room court stated, "protection . . . extends only to the limits that the design, purpose and plan of the public facility affords . . . .(125) Protection extends, therefore, to the conversations of customers in Dunkin' Donuts. They have a reasonable expectation of privacy because the design, purpose, and plan of a Dunkin' Donuts afford it.(126) The rationale of another fitting-room case, *Ohio v. McDaniel*,(127) further supports that expectation:

Even though the customer may be aware, and may be deemed to have consented, to the possible intrusion into her privacy by the inadvertence of another customer or by a salesclerk who intends to assist the customer, the customer using the fitting room has a reasonable expection [sic] that her privacy will not be invaded by an intruding eye from a concealed vantage point.(128)

Likewise, the customers of Dunkin' Donuts seek to preserve their conversational privacy in areas not totally closed off from the public. In so doing, they have a reasonable expectation that their privacy will not be invaded by an intruding ear that eavesdrops from a concealed vantage point. Accordingly, the objective prong of the "oral communication" test has been satisfied. Conversations held in a Dunkin' Donuts qualify as "oral communications" for purposes of Title III.

B. Does the Consent Exception Apply to the Interception of this Oral Communication?

As previously noted, Title III generally allows interceptions made when one party to the communication consents.(129) Dunkin' Donuts cannot claim party status to a private conversation between customers. Therefore, in order to lawfully intercept a communication, Dunkin' Donuts must obtain prior consent from any conversing party. Title III has been held to afford a safe harbor for interceptors acting with either explicit or implied consent.(130)

1. Adequate Notice and the Fitting-Room Standards

The second proposition evident from the fitting-room cases is the requirement of adequate notice of surveillance techniques before any implied consent can be imputed to the customer.(131) Adequate notice in the fitting-room context requires either a prominently placed warning,(132) or some obvious physical condition of the premises that would make a privacy expectation unreasonable.(133) Fitting-room cases focus upon knowledge available to the customer. Under this standard, Dunkin' Donuts has failed to provide the requisite notice to its customers.

Emphasizing knowledge available to the customer, the Texas Court of Criminal Appeals held that no expectation of privacy was violated by a department-store security officer who, while on all fours and peering under a fitting-room door, observed a customer place a sweater in her purse.(134) The reason, the court said, was a prominently placed surveillance notice:

[T]he posted sign on the mirror which would under nearly all circumstances be looked at by female occupants of a

fitting room was notice that one could not expect privacy. This room was for use by the public on conditions established by the business. If appellant did not want to use the fitting room under the posted conditions, she was not compelled to do so.(135)

Not surprisingly then, the lack of any surveillance notice affords an expectation of privacy to a shoplifter observed under similar circumstances.(136) Finally, the existence of prominently located surveillance warnings served to defeat the expectation of privacy by a civil complainant. In *Lewis v. Dayton Hudson Corp.*,(137) overhead surveillance by a same-sex security guard was not held to invade a customer's privacy when an undercover police officer was detained upon observation that he carried a gun in the fitting room.(138)

The notice provided by Dunkin' Donuts consisted of an entry-door sticker that advised "[a]udio monitoring on premises.(139) With good reason, the sufficiency of that "warning" has been questioned by at least one security systems provider,(140) as well as by the Consumer Protection Bureau of the New Hampshire Attorney General's Office.(141) According to Senior Assistant Attorney General Walter L. Maroney, the single small sticker utilized by Dunkin' Donuts was insufficient for two reasons. First, it was printed in English but used in two communities (Manchester and Concord) that have Spanish- and French-speaking populations. Second, the placement of the sticker was too far removed from the points of actual interception.(142) While Maroney's office does not issue written guidelines as to what constitutes sufficient notice, he does suggest that the warning would have to be "large enough that it would conceivably be seen" and placed "in real proximity to legitimate [interception] locations.(143)

A small sticker placed on the entry door of a Dunkin' Donuts hardly compares with the surveillance warning prominently displayed on individual fitting-room mirrors. Even assuming that customers actually see the notice and can read it, the advice "[a]udio monitoring on premises" is ambiguous at best. It does not inform customers that the conversations held in their individual booths are subject to electronic surveillance. Further, there is no open and obvious condition in a Dunkin' Donuts premises that would suggest to customers the existence of, or need for, audio surveil lance. As one customer in a Massachusetts Dunkin' Donuts commented about that store's video cameras: "There can't be anything in here worth stealing that's worth half the cost of those cameras.(144) Finally, whereas retail fitting rooms are known for their role in shoplifting capers, doughnut shop booths are not.

Under the fitting-room case standards, Dunkin' Donuts has failed to adequately warn customers about its use of electronic surveillance. Without that warning, customers have not given their implied consent to any electronic eavesdropping.

2. Adequate Notice and the Wire Communications Standards

While the standards established by cases involving wire communica tions have not been previously considered, they serve as a point of reference on the question of consent. In the case of wire communications, the safe harbor of Title III has been buttressed by the belief that Congress intended a broad construction of the consent requirement.(145) Notwith standing congressional intent, the prophylactic purpose of Title III suggests that consent should not be casually inferred.(146) Similar to the case of oral communications, a finding of implied consent for the interception of a wire communication will depend upon what reasonably constitutes adequate notice. Implied consent was found where an interceptor's repeated announcement of her intent to monitor all incoming calls gave the tenant/complainant "considerably more than a mere expectation that his call might, or probably would, be monitored.(147) Likewise, continued use of prison telephones by inmates who received notice of an interception policy from at least four sources constituted their implied consent to the monitoring.(148)

In contrast, implied consent has not been extended to the interception of an entire personal call where an employee expressly consented to the limited monitoring of her sales calls.(149) Similarly, there has been no implied consent to monitoring where the record did not reflect that an executive officer had been informed of either the manner in which the monitoring was to be conducted or that he personally would be moni tored.(150) Finally, no consent could be implied from circumstances reflecting that an employee suspected of burglary had knowledge only that her calls might or could be monitored, not that they actually would be.(151)

Applying these holdings to the case of Dunkin' Donuts reflects that even the broadest construction of the consent requirement does not support an inference of customer consent to the surveillance of personal table talk. At best, a

warning sticker on the premises door signifies the company's capacity for surveillance, not an intent to engage in it. Such circumstances have been held insufficient to imply consent by both the Eighth and Eleventh Circuits.(152) Nor does one sign on a general access door inform any particular customer that his or her conversations may be the target of surveillance or, in fact, how that surveillance would be conducted, as required by the First Circuit in *Williams*.(153) Even less tenable would be the suggestion that one "audio monitoring on premises" sign would instill in customers "considerably more than a mere expectation" that their conversations would be subjected to surveillance.(154) While the question is fact specific, the wire cases where consent has been implied from circumstances have involved "far more compelling facts(155) than the ones presented by Dunkin' Donuts. In the absence of valid claims of either party status or implied consent, the electronic surveillance performed by Dunkin' Donuts constitutes a prohibited interception within the meaning of Title III.

C. Has Dunkin' Donuts Intentionally Intercepted the Oral Communications of its Customers?

Both criminal and civil liability under Title III require intentional conduct by Dunkin' Donuts in its nonconsensual interception of oral communications.(156) Dunkin' Donuts has the requisite culpability to incur liability under the statute.

1. Intentional Conduct Requires a Conscious Objective

Title III's state-of-mind requirement resulted from an amendment to Section 2511(1)(a) by the Electronic Communications Privacy Act of 1986 (Privacy Act),(157) which substituted the word "intentionally" for "willful ly.(158) According to the legislative history of the Privacy Act, intentional conduct for Title III purposes requires a conscious objective to engage in the conduct or cause the result.(159) Intentional conduct is, therefore, the equivalent of purposeful conduct under the Model Penal Code.(160)

Senate Report No. 541 clearly states that the change in the required mental state from "willfully" to "intentionally" was meant to "underscore that inadvertent interceptions are not crimes under the Electronic Communi cations Privacy Act.(161) However, the Report further explains that the change in mental states "addresses the concerns of radio scanners that in the course of scanning radio frequencies in order to receive public communications, one could inadvertently tune through a protected communication like a cellular telephone call.(162)

Dunkin' Donuts suggested that it installed audio equipment to intercept only its employees' conversations.(163) Any other interceptions, Dunkin' Donuts might claim, were the product of inadvertence rather than intentional acts. As a result, they would not fall within the prohibitions of Section 2511(1)(a). The Dunkin' Donuts interceptions, however, do not fit within the categories of inadvertence suggested by the legislative history of the Privacy Act or the subsequent case law construing Title III.

Dunkin' Donuts installed equipment that had not only the capacity to record both employee and customer conversations but an inability to distinguish between them. Having done so, Dunkin' Donuts acknowledges the possibility that customer conversations could be intercepted as well.(164) While that might at first blush appear analogous to the situation of radio scanners, the difference lies in one critical fact: If Dunkin' Donuts made nonconsensual interceptions of employee conversations, it, unlike one scanning through radio frequencies, intentionally engaged in prohibited conduct at the time of the inadvertent interceptions. A lawsuit filed in New Hampshire on behalf of Dunkin' Donuts employees and customers alleges that employee conversations were, in fact, intercepted without consent.(165)

Title III simply will not allow Dunkin' Donuts to distinguish between contemplated and actual results. Senate Report No. 541 uses the disjunctive "or" when defining intentional conduct as being an objective purpose either to do an act or cause a harm.(166) If Dunkin' Donuts had the requisite intent to intercept oral communications without consent, it makes no difference that the "wrong" conversations—those of customers as opposed to employees—were actually intercepted. Nor does this fact affect the analysis under the Model Penal Code: It affords no legal significance to a divergence between actual and contemplated results when the only consequence of the divergence is that a different person or property has been affected.(167) Accordingly, a claim of inadvertence as to the particular conversations intercepted by Dunkin' Donuts has no legal significance as it relates to the requisite state of mind under Section

2511(1)(a).

Further, the Dunkin' Donuts scenario does not establish the kind of inadvertence protected in the case of *Sanders v. Robert Bosch Corporation*, where an unknown design defect in a telephone voice logger resulted in the microphone transmission of telephone and other conversations after the logger had been deactivated.(168) Dunkin' Donuts cannot claim inadver tence to defeat the intent element of Section 2511(1)(a).

2. Intentional Conduct Does Not Consider Underlying Motive

Neither can Dunkin' Donuts rely upon a lack of bad purpose to escape liability under Title III. While willful conduct took into account the interceptor's motive, intentional conduct does not, as evidenced by the legislative history of the Privacy Act. Senate Report No. 541 states, "Liability for intentionally engaging in prohibited conduct is not dependent on an assessment of the merit of the motive . . . .(169) Thus, intent refers only to the actor's state of mind in making the interceptions. In this respect, the Privacy Act signifies a change in the required mental state by substituting "intentionally" for "willfully.(170)

Senate Report No. 1097, which accompanied Title III as enacted, referred to the Supreme Court's standard for willful conduct in the criminal context.(171) Under the *Murdock* standard, "[W]hen used in a criminal statute, it [willful] generally means an act done with a bad purpose; without justifiable excuse; stubbornly, obstinately, perversely.(172) Thus, the concept of willful behavior as defined by some courts included a consider ation of the underlying motive.(173) For those courts, willful conduct meant intent plus a bad purpose. That a willful state of mind could require an undesirable motive receives support from cases where the triers of fact found intentional interceptions but no willful behavior. This lack of a willful component to an intentional act of interception developed in cases of spousal wiretapping when the intercepting party believed in the legality of his or her actions.(174) While Dunkin' Donuts has claimed such a belief,(175) it was not formed upon the advice of legal counsel.(176) Nor is that belief relevant to the inquiry of "intentional" interceptions under Section 2511(1)(a).(177)

Regardless of its motive in intercepting conversations or its belief in the legality of those interceptions, Dunkin' Donuts evinces the requisite intent under Section 2511(1)(a). For Title III purposes, Dunkin' Donuts intentionally intercepted its customers' conversations.

V.Problems with Title III Enforcement

This Note demonstrates that the audio surveillance employed by Dunkin' Donuts and similar businesses violates the letter and spirit of Title III. Unfortunately, the discovery of surreptitious audio surveillance does not guarantee that the statutory prohibitions will be enforced.

After the enactment of Title III, Congress established a National Wiretap Commission (Commission) to study its enforcement. A 1976 Report of the Commission found that the enforcement of Title III against private actors proved difficult for reasons that still exist today.(178) Those reasons include (1) victim reluctance to report offenses and incur additional privacy losses; (2) judicial reluctance to apply Title III's severe civil penalties; (3) jury reluctance to convict individuals who claim as their motivation a desire to uncover wrongdoing; and (4) the shortage of enforcement personnel.(179) In addition, the obstacle imposed by the judicial system in its narrow interpretation of the statute has not been removed.(180) As a result, Title III's enforcement was, and still is, "disap pointing.(181)

Congress has yet to amend Title III, as the Commission suggested, to include misdemeanor penalties "to encourage conviction by ambivalent juries.(182) However, Congress has significantly increased the amount of civil damages recoverable under Title III, which the Commission recommended to "encourage individual lawsuits against violators.(183) While such lawsuits may now be encouraged, it remains unclear that they will produce a corresponding benefit to the plaintiffs who initiate them.

The Privacy Act significantly amended the provisions for civil damages under Section 2520 by increasing the minimum statutory damages from $1000 to $10,000 for violations other than certain satellite video communications offenses.(184) Section 2520 now provides:

(2) [T]he court *may* assess as damages whichever is the greater of—(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.(185)

Accompanying that increase in statutory damages, however, came a change from the mandatory "shall" to the permissive "may" in the trial court's directive.(186) In response, the circuits have split on whether courts now have the discretion to decline an award of damages.(187) The majority view clearly favors trial court discretion, but neither interpretation bodes well for the effective enforcement of Title III. Under the majority view, those courts reluctant to impose hefty civil damages now have the option to award only actual damages—which are often *de minimis*—or none at all. While that option could lead to more plaintiffs' verdicts, such a victory remains hollow at best. The possibility of a zero or negligible dollar judgment provides little incentive to plaintiffs and even less deterrent to those who would engage in prohibited surveillance. Further, plaintiffs must litigate in courts having the discretion to conclude that a damage award "would serve no purpose.(188) On the other hand, the minority view exacerbates the problem of judicial reluctance, particularly now that the civil penalties have been greatly enhanced.

This leaves only the normal prosecutorial policy of responding to complaints of illegal eavesdropping, which the Commission found unsatisfactory.(189) While such a policy appears to have succeeded in the case of Dunkin' Donuts, the public cannot rest assured that all inquiries will result in similar cooperation. Local Dunkin' Donuts franchisees reportedly ceased their audio surveillance within hours of a request made by the New Hampshire Attorney General's Office.(190) Yet even in its cooperation, Dunkin' Donuts exemplifies the lawlessness associated with covert audio surveillance in such businesses. Dunkin' Donuts Incorporated knew nothing about the use of audio surveillance in its franchises until the newspaper stories appeared, according to company spokesman William Chiccarelli.(191) Dunkin' Donuts Incorporated responded to those media reports by sending a Western Union Mailgram "requesting that all franchisees with such audio devices disconnect and remove the devices from their shops.(192) Corporate Dunkin' Donuts offered the public a mere request that its franchisees desist from using audio surveillance. Worse yet, that request is one with which franchise owners have no obligation to comply.(193)

Despite the statutory prohibitions, enforcement difficulties have rendered Title III ineffective in pulling the plug on private-sector bugs.

Conclusion

Dunkin' Donuts and similar businesses offer three reasons for their use of covert audio surveillance: (1) to monitor customer service,(194) (2) to prevent quick-change scams,(195) and (3) to keep employees from pocketing a quarter here and there.(196) While these remain valid manage ment objectives, they hardly compare to the serious crime for which Title III authorizes court-approved interceptions by law enforcement.(197) Title III established national standards to be strictly construed by the courts. It also established a blanket prohibition, with three specific exceptions, upon electronic surveillance performed by anyone other than authorized law enforcement. Businesses such as Dunkin' Donuts do not satisfy any of those exceptions, and Congress did not intend otherwise.

However, some twenty-five years after the enactment of Title III, electronic surveillance invades the public spheres of daily life. As G. Gordon Liddy said of the Watergate break-in, "[S]urveillance is like brushing your teeth . . . . It's basic.(198) It is so basic—and insidious— that the subject of an interception often remains unaware of the intrusion. The audio surveillance at Dunkin' Donuts emphasizes this point. Mere happenstance, in the form of curiosity from a hungry investigator, brought the prohibited practices to light.

This knowledge offers no comfort to the customers who visit their neighborhood Dunkin' Donuts for a cup of dark-roast coffee and perhaps one of corporate America's favorite jelly-filled doughnuts.(199) They may derive some solace, however, from the fact that the New Hampshire Attorney General's Office found no evidence of surveillance abuse during its Dunkin' Donuts investigation.(200) Still, one favorable report will not quash the fears that arise from the mere suggestion that the contents of private coffee klatches have been picked up by a furtive bug and carried to a remote location where unseen managers and even employees can overhear them.(201) That mere suggestion appeared to be grounded in fact when a former three-year employee of a Manchester, New Hampshire, Dunkin' Donuts told the media that she and fellow employees eavesdropped on customers' coffee talk, especially when it concerned intimate

details about people they knew. Admitting that those details were circulated throughout the store, Tammy O'Neal, who was fired in 1992, said eavesdropping employees "would make fun of people's private lives.(202)

Before they resort to breaking the law with covert electronic surveillance, businesses should consider the words of former President Richard Nixon. Discussing the practice of wiretapping with John Dean, Nixon offered some hindsight applicable here: "They [the taps] never helped us. Just gobs and gobs of material: gossip and bullshitting . . . .(203) The practice of electronic spying connotes a war mentality that not only thinks in terms of enemies,(204) but which mocks the philosophy of Dunkin' Donuts and similar establishments. "We're in the business of satisfying customers," said Chiccarelli.(205) Those customers, he noted, have expressed their concern about the surveillance.(206)

Customers express their concern with good reason. Spy gear has become a multimillion-dollar industry that provides the public with access to increasingly smaller and more powerful equipment once available only to law enforcement.(207) For those businesses that choose to utilize such equipment, they can do so lawfully by providing notice sufficient to establish consent. This does not mean a warning sticker that is "roughly one-third of the size of the sign" directly above it that reads "No shirt, no shoes, no service.(208) Rather, it means a sign that will capture the customer's attention. When it does just that, businesses can listen to the sound of silence as customers take their patronage elsewhere.

Bugs are a filthy business indeed. The dirt they carry has no place in a doughnut shop.

(1)†*See* Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The*

Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop, 41 DePaul L. Rev. 739, 770, n.161 (1992) (discussing a July 3, 1990 telephone interview with Lou Gerber, legislative director of the Communications Workers of America, who said that many employers appear to have as their motto, "In God we trust. Others we monitor.")

(1)* B.A. (English) with high distinction, B.A. (Journalism) with high distinction, Indiana

University—Bloomington, 1993; candidate for J.D. Indiana University School of Law—Bloo mington, December 1995. My special thanks to David Schwartz for his encouragement; to James Louis Calamaras Professor of Law Craig M. Bradley and Associate Professor of Law Fred H. Cate for their constructive comments; and to Ginger and her father for their continued moral support throughout law school.

(1)" . Hillary Chura, *Fly in Your Soup? How About a Bug in Your Booth?*, L.A. Times

(Bulldog Ed.), May 29, 1994, at A2.

(2). Randolph Ryan, *Legality of Hidden Mikes at Businesses Questioned*, Boston

Globe, May 27, 1994, at 1. On May 26, the *Concord Monitor* first reported the installation of audio surveillance systems at hundreds of Dunkin' Donuts stores. Tom Coakley & Sean P. Murphy, *Dunkin' Donuts to Stop Recording*, Boston Globe, May 28, 1994, at 1, 6. A New Hampshire security firm was credited with the installation of 500 systems in restaurants and businesses across the Northeast. *Id.* at 6.

(3). Ryan, *supra* note 2, at 1.

(4)" . Chura, *supra* note 1, at A2.

(5). Peter T. Kilborn, *In a Growing Number of Stores, Hidden Security Microphones Are*

Listening, N.Y. Times, May 28, 1994, at A6.

(6). *Id.* McDonald's apparently declines to follow the trend. "It [audio surveillance] is

just not something that we do," said company spokeswoman Ann Connolly. *Id.*

(7). *Id.*

(8). Chura, *supra* note 1, at A2.

(9). *Id.*

(10). The term "bug" denotes a hidden microphone that intercepts conversations and

other sounds occurring in a given space, as distinguished from a wiretap, which intercepts telephone conversations occurring on a given line. Both bugs and wiretaps allow the interceptor to overhear and record conversations from a remote location. *See* Herman Schwartz, Taps, Bugs, and Fooling the People 19 (1977).

(11). *Equipment Demand Grows*, Sec. Mgmt., Sept. 1994, at 20, 20 (quoting Edward

Hester, Study #591 Security Surveillance & Monitoring).

(12). *Id.*

(13). *Id*.

(14). Surveillance in the workplace connotes general "observation to determine employee

behaviors and personal characteristics." It is distinguished from workplace monitoring, which is undertaken to determine whether an employee has completed an assigned task appropriately. Robert G. Boehmer, *Artifical Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DePaul L. Rev. 739, 749 (1992).

(15). 18 U.S.C.A. §§ 2510-2520 (West 1988 & Supp. 1995).

(16). United States v. Capra, 501 F.2d 267, 276 (2d Cir. 1974), *cert. denied*, 420 U.S.

990 (1974).

(17). *Id.*

(18). Those four states are Mississippi, Missouri, South Carolina, and Vermont. Bureau

of Justice Statistics, U.S. Dep't of Justice, Sourcebook of Criminal Justice Statistics—1992 159 (1992).

(19). N.H. Rev. Stat. Ann. § 570-A:2 (1994). This statute provides that a third party

who intercepts an oral or wire communication without the consent of all parties to the communication commits a class B felony. *Id.* Section 570-A:2 requires the consent of *all* parties to the communication, whereas Title III requires the consent of only one party. *Id. See* 18 U.S.C. § 2511(2)(d) (1994).

(20)" . *Tiny ears may be listening: Stores plant mikes as anti-theft devices*, Sun Sentinel

(Fort Lauderdale), May 28, 1994, at 3A.

(21). *See Surveillance Countermeasures*, Sec. Mgmt., Oct. 1994, at 26, 26 (advertising

surveillance countermeasure products).

(22). Agreement Letter from Matthew Donuts, Inc., to Jeffrey R. Howard, New

Hampshire Attorney General 1 (June 1, 1994) [hereinafter Agreement Letter] (on file with the State of New Hampshire, Department of Justice, Office of the Attorney General, Concord, N.H.).

(23). *Id.* at 1-2.

(24). *Id.* at 1.

(25). *Id.* at 2.

(26). *Id.*

(27). *Id.*

(28). Telephone Interview with Walter L. Maroney, Senior Assistant Attorney General,

Consumer Protection and Antitrust Bureau, Office of the Attorney General for the State of New Hampshire (Aug. 10, 1995).

(29). *Id.*

(30). *Id.*

(31). *Id.*

(32). Teresa Anderson, *Legal Reporter*, Sec. Mgmt., Dec. 1994, at 70, 73.

(33). H.R. 1900, 103d Cong., 1st Sess. (1993).

(34). S. 984, 103d Cong., 1st Sess. (1993).

(35). Read Hayes, *Passage of employee monitoring bill would be a true loss,* Discount

Store News, May 16, 1994, at 118, 118.

(36). The Security Companies Organized for Legislative Action (SCOLA) petitioned the

Senate for a total security exemption that would exclude practices designed to protect employees and property. Teresa Anderson, *Is Electronic Monitoring Getting the Plug Pulled?,* Sec. Mgmt., Oct. 1993, at 73, 73.

(37). Restaurants and convenience stores insisted upon having the ability to collect and

compare point-of-sale data. Pat Williams, *Privacy bill to limit, not prohibit, electronic surveillance in marketplace*, Discount Store News, May 16, 1994, at 120, 120.

(38). H.R. 1900 § 9(a)(2) (emphasis added).

(39). H.R. 1900 § 4(e).

(40)" . *ASIS Gives Congress Statement on Bill*, Sec. Mgmt., Nov. 1993, at 64, 64.

(41). Omnibus Crime Control and Safe Streets Act of 1968, S. Rep. No. 1097,

90th Cong., 2d Sess. 56 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.

(42)" . *Id.* at U.S.C.C.A.N. 2154.

(43). *Id.*

(44). *Id.* at U.S.C.C.A.N. 2153.

(45). *Id.* at U.S.C.C.A.N. 2157.

(46). *Berger*, 388 U.S. 41 (1967) (holding a New York eavesdropping statute to be

facially unconstitutional because it lacked particularity as to the crime being investigated, the location to be searched, and the "things" to be seized. The majority felt that the obtrusive nature of eavesdropping made the need for specificity "especially great." *Id*. at 56, 58-60.).

(47). *Katz*, 389 U.S. 347 (1967) (holding that the Fourth Amendment protects people,

not merely places, and, thus, a lack of physical intrusion into a given enclosure will not defeat a justifiable expectation of privacy against the interception of communications. Katz was held to have such an expectation in the public telephone booth from which he transmitted wagering information and to the outside of which FBI agents had attached a listening-and-recording device. *Id*. at 353. Prior Supreme Court decisions required a physical trespass before evidence obtained through law-enforcement eavesdropping could be suppressed as the fruits of an illegal search and seizure. *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928) and Goldman v. United States, 316 U.S. 129 (1942)).

(48)" . S. Rep. No. 1097, *supra* note 41, at U.S.C.C.A.N. 2153 (emphasis added).

(49)" . *Invasions of Privacy: Hearings Before the Subcomm. on Admin. Prac. & Proc. of*

the Senate Comm. on the Judiciary, 89th Cong., 2d Sess., 2261 (1966)

(50)" . S. Rep. No. 1097, *supra* note 41, at U.S.C.C.A.N. 2156.

(51). 18 U.S.C. § 2511(1)(a)-(e) (1994).

(52). 18 U.S.C. § 2511(4)(a) (1994).

(53). 18 U.S.C. § 2520(a)-(c) (1994).

(54). 18 U.S.C. § 2515 (1994).

(55). 18 U.S.C. § 2512 (1994).

(56). 18 U.S.C. § 2511(2)(c)-(d) (1994).

(57). 18 U.S.C. § 2511(2)(c) (1994).

(58). 18 U.S.C. § 2511(2)(d) (1994).

(59). 18 U.S.C. §§ 2516, 2518 (1994).

(60). 18 U.S.C. § 2511(2)(a)(i) (1994).

(61). 18 U.S.C. § 2511(2)(b) (1994).

(62). 18 U.S.C.A. § 2511(2)(e)-(f) (West 1988 & Supp. 1995).

(63)" . Angel v. Williams, 12 F.3d 786, 789 n.5 (8th Cir. 1993).

(64). *Id.*

(65)" . 18 U.S.C. § 2510(2) (1994).

(66). *Angel*, 12 F.3d at 790.

(67). *Katz*, 389 U.S. 347 (1967).

(68)" . *Id.* at 361 (Harlan, J., concurring).

(69). *Angel*, 12 F.3d at 790.

(70). 18 U.S.C. § 2510(2) (1994).

(71). *Id.*

(72)" . 18 U.S.C. § 2510(2) (1994) (emphasis added). *See supra* text accompanying note

65.

(73)" . United States v. Turkette, 452 U.S. 576, 580 (1981) (rejecting application of the

rule of lenity to an unambiguous RICO statute, 18 U.S.C. § 1962).

(74)" . 18 U.S.C. § 2510(4) (1994).

(75). "`When I use a word,' Humpty-Dumpty said in a rather scornful tone, `it means

just what I choose it to mean—neither more nor less.'" Kratz v. Kratz, 477 F. Supp. 463, 470 n.12 (E.D. Pa. 1979) (quoting Lewis Carroll, Through the Looking-Glass and What Alice Found There 274 (Puffin Books 1962) (1871)).

(76). *Walker*, 911 F.2d 1573 (11th Cir. 1990).

(77)" . *Id.* at 1578-79.

(78). *Id.*

(79). Wesley v. WISN Division—Hearst Corp., 806 F. Supp. 812, 814-15 (E.D. Wis.

1992) (holding no reasonable expectation of noninterception by a former radio station account executive who conversed with a traffic reporter near a microphone at the reporter's work station. The district court found that the existence and position of the microphone were sufficient to put Wesley "on notice that her comments might be intercepted.").

(80). Angel v. Williams, 12 F.3d 786, 790 (8th Cir. 1993).

(81). *Id.*

(82). *See* S. Rep. No. 1097, *supra* note 41, at U.S.C.C.A.N. 2178 (stating that an

expectation of noninterception would be "unjustified in certain areas; for example a jail cell").

(83). United States v. Harrelson, 754 F.2d 1153 (5th Cir. 1985), *reh'g denied*, 766 F.2d

186 (5th Cir. 1985), *cert. denied*, 474 U.S. 908 (1985), *cert. denied*, 474 U.S. 1034 (1985) (holding that conversations between a husband and his wife during a jail visit were not "oral communications" under Title III and could be

admitted into evidence. The interceptions were performed by a prisoner in an adjoining cell, who acted on behalf of the FBI). *See also* People v. Siripongs, 754 P.2d 1306 (Cal. 1988) (en banc) (holding that a murder defendant had no reasonable expectation of privacy during a telephone conversation conducted in Thai, when a police officer stood beside him during the call, nor a reasonable expectation that the officer would not record the call for later translation), *cert. denied,* 488 U.S. 1019 (1989).

(84). *Angel*, 12 F.3d at 790 (holding that city police officers who were terminated for

using excessive force on a prisoner could not prevail in their civil action against the city for unlawful interception because the tape-recorded incident in question occurred within a public jail. "These are the only material facts necessary to prove, as a matter of law, that it was not objectively reasonable for the officers to expect that their conversations would not be intercepted." *Id*.).

(85) . Kerry Hannon, *Two doughnuts and a martini, please*, Forbes, Mar. 9, 1987, at

128, 130.

(86). Seth Lubove, *Coffee versus Gazebo Blend*, Forbes, June 20, 1994, at 112, 112.

As the nation's largest retailer of doughnuts and freshly brewed coffee, Dunkin' Donuts experienced 15 consecutive years of increased revenues and earnings prior to its 1989 takeover by Allied-Lyons Plc., a British distiller. *Id*.

(87). *Id.*

(88)" . *Id.* (quoting Jack Shafer, president of Dunkin' Donuts U.S.A.).

(89). Ryan, *supra* note 2, at 1.

(90). *See* U.S. Const. amend. IV, which provides that "[t]he right of the people to be

secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."

(91). *See Katz*, 389 U.S. 347, 353 (1967).

(92)" . *Id.* at 351-52.

(93)" . *Id.* at 361 (Harlan, J., concurring).

(94). *In re* John Doe Trader Number One, 894 F.2d 240, 245 (7th Cir. 1990).

(95). *Id.*

(96). Louis B. Schwartz, *On Current Proposals to Legalize Wiretapping*, 103 U. Pa. L.

Rev. 157, 162-67 (1954).

(97)" . United States v. White, 401 U.S. 745, 777 (1971) (Harlan, J., dissenting), *reh'g*

denied, 402 U.S. 990 (1971).

(98)" . Ralph S. Spritzer, *Electronic Surveillance by Leave of the Magistrate: The Case*

in Opposition, 118 U. Pa. L. Rev. 169, 169 (1969) (quoting 4 W. Blackstone, Commen taries *168).

(99)" . Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting),

overruled by Florida v. Riley, 488 U.S. 445 (1989).

(100). 401 U.S. 745 (1971).

(101). *Id.* at 746-47 (plurality opinion) (holding that a criminal defendant's Fourth Amend

ment rights were not violated by the admission of testimony from two narcotics agents, in lieu of testimony from a missing informant, as to contents of conversations that occurred between the defendant and the informant, in the informant's home. Those conversations were monitored by the agents with the informant's consent through the use of a radio transmitter concealed on the informant and by one agent having been concealed in a closet).

(102). *Id.* at 787 (Harlan, J., dissenting).

(103)" . *Id*.

(104). Schwartz, *supra* note 96, at 162.

(105). R. Kent Greenawalt, *Privacy and Its Legal Protection*, 2 Hastings Center Stud.

45, 50, 59-60 (1974) *reprinted in* Monrad G. Paulsen, The Problems of Electronic Eavesdropping 6-11 (1977).

(106). *Id.*

(107)" . Spritzer, *supra* note 98, at 180.

(108). *Id*.

(109). Don Mayer, *Workplace Privacy and the Fourth Amendment: An End to Reasonable*

Expectations?, 29 Am. Bus. L.J. 625 (1992).

(110)" . *Id.* at 637.

(111). Smith v. Maryland, 442 U.S. 735 (1979) (upholding the placement, without a

warrant, of a "pen register" to record numbers dialed from defendant's telephone).

(112). California v. Greenwood, 486 U.S. 35, 40 (1988) (upholding warrantless search of

garbage for evidence of narcotics use because "bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public").

(113). California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (upholding search warrant

obtained based upon police officer's observation of crop from a private plane flying at 1000 feet over defendant's house. The Court concluded that "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers ob served"). *See also* Florida v. Riley, 488 U.S. 445 (1989) (upholding search warrant obtained based upon state agent's observance of greenhouse-concealed marijuana crop from a helicopter flying at 400 feet).

(114). *Dow Chemical*, 476 U.S. 227 (1986).

(115)" . *Id.* at 238. The Court also based its denial upon the "open fields" exception, which

limits Fourth Amendment protection to areas within the "curtilage" of a premises. *Id.* at 235-39.

(116). Mayer, *supra* note 109, at 643.

(117)" . *Id.* at 660.

(118). *Id*.

(119). 18 U.S.C. § 2511(2)(d) (1994). *See supra* notes 56-58 and accompanying text.

(120). *Katz*, 389 U.S. 347, 351-52 (1967).

(121). *In re Deborah C.*, 635 P.2d 446, 452 (Cal. 1981) (en banc).

(122). 635 P.2d 446 (Cal. 1981).

(123). *Id.* at 451.

(124)" . *Id.* at 452.

(125)" . Gillett v. Texas, 588 S.W.2d 361, 363 (Tex. Crim. App. 1979).

(126). *Cf. Id.*

(127). *McDaniel*, 337 N.E.2d 173 (Ohio Ct. App. 1975).

(128). *Id.* at 177.

(129). 18 U.S.C. § 2511(2)(d) (1994). *See supra* notes 56-58 and accompanying text.

(130). Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990).

(131). *McDaniel*, 337 N.E.2d at 173.

(132). Gillett v. Texas, 588 S.W.2d 361, 363 (Tex. Crim. App. 1979). *See also*

McDaniel, 337 N.E.2d at 173.

(133). *In re Deborah C.*, 635 P.2d 446 (Cal. 1981) (en banc).

(134). *Gillett*, 588 S.W.2d at 363.

(135). *Id.*

(136). *McDaniel*, 337 N.E.2d at 173.

(137). *Lewis*, 339 N.W.2d 857 (Mich. Ct. App. 1983).

(138). *Id.* at 858, 860-61.

(139)" . Kilborn, *supra* note 5, at A6.

(140). According to Jeffrey Meuse, owner of National Security Video, Inc., of Goffstown,

New Hampshire, manufacturers of the surveillance equipment enclose notice stickers in their shipments. "The question," Meuse said, "is whether the stickers are noticed." *Id.*

(141). Telephone Interview with Walter L. Maroney, *supra* note 28.

(142). *Id.*

(143)" . *Id.*

(144)" . Ryan, *supra* note 2, at 24 (quoting customer Rick Foster of Hyde Park, Massachusetts).

(145). United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987), *cert. denied*, 485 U.S. 1021 (1988). *Accord* Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1981).

(146). *Griggs-Ryan*, 904 F.2d at 117. *See also* Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).

(147)" . *Griggs-Ryan*, 904 F.2d at 118.

(148). *Amen*, 831 F.2d at 379.

(149). *Watkins*, 704 F.2d at 581.

(150). Williams v. Poulos, 11 F.3d 271, 281-282 (1st Cir. 1993).

(151). Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992).

(152). *See Watkins*, 704 F.2d at 581. *See also Deal*, 980 F.2d at 1157.

(153). *Williams,* 11 F.3d at 281-82.

(154). *See* Griggs-Ryan v. Smith, 904 F.2d 112, 118 (1st Cir. 1981).

(155)" . *Watkins*, 704 F.2d at 581.

(156). 18 U.S.C. § 2511(1)(a) (1994).

(157). Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

(158)" . *Id*. at § 101(f), 100 Stat. 1853.

(159). S. Rep. No. 541, 99th Cong., 2d Sess., 23 (1986), *reprinted in* 1986 U.S.C. C.A.N. 3555, 3577.

(160). (a) *Purposely.* "A person acts purposely with respect to a material element of an offense when:

(i) if the element involves the nature of his conduct or a result thereof, it is his conscious object to engage in conduct of that nature or to cause such a result." Model Penal Code § 2.02(2)(a) (Official Draft 1962).

(161)" . S. Rep. No. 541, *supra* note 159, at U.S.C.C.A.N. 3577.

(162)" . *Id.* at U.S.C.C.A.N. 3560.

(163). *See* Agreement Letter, *supra* note 22, at 2.

(164). *Id.*

(165). Hodgdon v. Dunkin' Donuts, No. 94-C-00868 (N.H. Super. Ct. for the N. Dist.

of Hillsborough County filed Aug. 5, 1995) [hereinafter *Hodgdon*] (Class action suit filed on behalf of two former Dunkin' Donuts employees and various customers alleging non consensual interceptions of both employee and customer conversations in New Hampshire stores. Settlement pending pursuant to Aug. 29, 1995 docket entry.).

(166). S. Rep. No. 541, supra note 159, at U.S.C.C.A.N. 3577.

(167). Section (2)(a) provides:

(2) When purposely or knowingly causing a particular result is an element of an offense, the element is not established if the actual result is not within the purpose or the contemplation of the actor unless:

(a) the actual result differs from that designed or contem plated, as the case may be, only in the respect that a different person or different property is injured or affected . . . .

Model Penal Code § 2.03 note on subsection (2)(a) (Official Draft 1962).

(168). *Sanders*, 38 F.3d 736, 742-43 (4th Cir. 1994), *reh'g denied*, No. 93-2423, 1995

U.S. App. LEXIS 1439 (4th Cir., Jan. 24, 1995) (en banc).

(169)" . S. Rep. No. 541, *supra* note 159, at U.S.C.C.A.N. 3578.

(170)" . Under the Model Penal Code, "willfully" means "knowingly," absent a legislative

purpose to impose further requirements. Model Penal Code § 2.02 explanatory note for subsection (8) (Official Draft 1962). As will be seen, some courts have found a legislative purpose to impose a motive requirement.

(171). S. Rep. No. 541, *supra* note 159, at U.S.C.C.A.N 3577-78.

(172)" . United States v. Murdock, 290 U.S. 389, 394-95 (1933) (cited in Citron v. Citron,

722 F.2d 14, 16 (2d Cir. 1983), *cert. denied*, 466 U.S. 973 (1984) (holding that the

criminal standard of willfulness, and its traditional meaning, would apply in both criminal and civil contexts alike). *See also* Malouche v. JH Management Co., 839 F.2d 1024, 1025- 26 (4th Cir. 1988).

(173). *See, e.g.,* United States v. Townsend, 987 F.2d 927, 931 (2d Cir. 1993) (upholding

the conviction of an Orange County, Vermont, sheriff for the nonconsensual interception of his employees' telephone conversations. The court concluded that amended Section 2511(1)(a) "only requires intentional interception of communications, *not willful intercep tion. The question of whether the defendant had a good or evil purpose . . . is, therefore, irrelevant.*") (emphasis added).

(174). *See* Farroni v. Farroni, 862 F.2d 109, 110-11 (6th Cir. 1988) (holding that a

husband's secret recordings of his wife's telephone conversations with third parties were intentional but not willful interceptions due to his belief that his actions were lawful. The Sixth Circuit affirmed judgment for the husband in this action by his wife for civil damages under § 2520.) *See also* Citron v. Citron, 722 F.2d 14, 14-15. In both cases, the intercepting parties sought and relied upon the advice of legal counsel.

(175). *See* Agreement Letter, *supra* note 22, at 1.

(176). *Id.*

(177). Unlike § 2511(1)(a) and (b), §§ 2511(1)(c) and (d) prohibit intentional disclosure

and use respectively of the contents of an intercepted communication. Those sections, as written and construed, require a greater degree of knowledge by the defendant than does § 2511(1)(a). They require as an element of the offense that the defendant knew or should have known facts that would suggest the illegal nature of the interception. Forsyth v. Barr, 19 F.3d 1527, 1538, n. 21 (5th Cir. 1994), *cert. denied,* 115 S. Ct. 195 (1994). Motive, however, is no longer a consideration under these sections.

(178). National Commission for the Review of Federal and State Laws

Relating to Wiretapping and Electronic Surveillance, 1976 Electronic Surveillance Report (1976) [hereinafter NWC Report].

(179). *Id.* at 23.

(180). *Id.* at 24.

(181)" . *Id.* at 23.

(182)" . *Id.* at xviii.

(183)" . *Id.*

(184). 18 U.S.C. § 2520(c)(2) (1994).

(185). *Id.* (emphasis added).

(186). S. Rep. No. 541, *supra* note 159, at U.S.C.C.A.N. 3581.

(187). *See*, *e.g.*, Nalley v. Nalley, 53 F.3d 649, 652 (4th Cir. 1995) (holding that the

change from a mandatory to permissive verb form signaled congressional intent that trial courts have the discretion to award or decline damages to civil plaintiffs under § 2520 (c)(2)). *But see* Rodgers v. Wood, 910 F.2d 444, 448 (7th Cir. 1990), *reh'g denied,* 914 F.2d 260 (1990) (refusing to "infer that Congress intended to increase the penalties for violations, but to permit defendants to escape the increased penalties if their actions did not warrant too severe a sanction." *Id.*).

(188)" . *Nally*, 53 F.3d at 654 (refusing to award damages against a wife who intercepted

her husband's telephone calls to another woman and then played the tape recordings for the couple's children, the other woman's husband, and the plaintiff's attorney).

(189). NWC Report, *supra* note 178, at 23.

(190). Telephone Interview with Walter L. Maroney, *supra* note 28.

(191). Coakley & Murphy, *supra* note 2, at 6.

(192)" . Letter from Catherine Spalding, Staff Attorney for Dunkin' Donuts Incorporated,

to Walter Marone [sic], Assistant Attorney General, New Hampshire Consumer Protection

Division, (May 27, 1994) (on file with the State of New Hampshire, Department of Justice, Office of the Attorney General, Concord, NH).

(193). *Dunkin' Donuts routinely eavesdropped*, Houston Post, May 29, 1994, at A10.

However, Chiccarelli indicated his belief that "with all the adverse publicity, we are confident they will comply." *Id.*

(194). Telephone Interview with Walter L. Maroney, *supra* note 28.

(195). *Id.*

(196). Kilborn, *supra* note 5, at 6.

(197). *See* 18 U.S.C. § 2516 (1994). At the state level, for example, application for

interception may be made by law enforcement in cases involving evidence of murder, kidnapping, robbery, extortion, bribery, gambling, dealing in narcotics, and other felonies "dangerous to life, limb, or property." *Id.* at § 2516(2).

(198)" . Schwartz, *supra* note 10, at 43 (quoting G. Gordon Liddy's conversation with

Mike Wallace).

(199). The next five national favorites for corporate America are honey-dipped, chocolate

honey-dipped, plain, "kreme," and chocolate frosted. Robert A. Mamis, *Doughnut Figures*, Inc., Oct. 1993, at 48, 48.

(200). Telephone Interview with Walter L. Maroney, *supra* note 28.

(201). Dallas Gatewood, *Now Big Brother Is Listening, Too. Store surveillance raises*

concern, Newsday, May 28, 1994, at A17.

(202)" . *Id.* Tammy O'Neal is a plaintiff in the Hodgdon lawsuit. *See Hodgdon*, *supra* note

165.

(203)" . *See* Schwartz, *supra* note 10, at 39.

(204). *Id*. at 43.

(205). Coakley & Murphy, *supra* note 2, at 6.

(206). *Id.*

(207). James C. McKinley, Jr., *U.S. Agents Raid Stores in 24 Cities to Seize Spy Gear*,

N.Y. Times, Apr. 6, 1995, at A1, B5.

(208)" . *Hodgdon*, *supra* note 165.