12-1-2005

United States v. Lifshitz: Warrantless Computer Monitoring and the Fourth Amendment

Shauna Curphey

UNITED STATES V. LIFSHITZ: WARRANTLESS COMPUTER MONITORING AND THE FOURTH AMENDMENT

I. INTRODUCTION

In *United States v. Lifshitz*,[1] the Second Circuit held that the Fourth Amendment to the United States Constitution protects probationers from overbroad computer monitoring as a condition of probation.[2] The defendant in *Lifshitz* claimed that warrantless, state-imposed computer monitoring, on its face, infringed his right to be free from unreasonable searches.[3] Thus, the court had to determine whether the state, without any suspicion of wrongdoing, could monitor a probationer's computer use without running afoul of the Fourth Amendment.[4] The court resolved the issue by comparing computer monitoring to random drug testing.[5] In doing so, the court did not focus on computers as a medium.[6] Instead, the court evaluated the content of the computer monitoring policy. As a result, the court demanded that the search condition be narrowly tailored to meet the state's needs without "sweep[ing] so broadly as to draw a wide swath of extraneous material into its net."[7]

The *Lifshitz* opinion rests on the jurisprudence of "special needs" searches.[8] The Fourth Amendment assures the right of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[9] In most cases, the

[1] 369 F.3d 173, 193 (2d Cir. 2004).

[2] *Id.*

[3] *Id.* at 175.

[4] *Id.* at 182.

[5] *Id.* at 183–87.

[6] *Id.* at 183.

[7] *Id.* at 190.

[8] *Id.* at 193.

[9] U.S. CONST. amend. IV. Fourth Amendment protection extends beyond the criminal justice context to all government searches. New Jersey v. T.L.O., 469 U.S. 325, 335 (1985), including those conducted by public school

Fourth Amendment's demand for reasonableness requires a valid warrant or a showing of probable cause before the state conducts a search.[10] However, courts allow exceptions when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[11] Courts determine the validity of a special needs search by weighing an individual's expectation of privacy against the government's interest in foregoing "a warrant or some level of individualized suspicion."[12] It was this balancing that led the court in *Lifshitz* to demand that the state's computer monitoring be narrowly tailored to its objective for the search.[13]

The imposition of computer or Internet restrictions as conditions of community supervision is on the rise.[14] Some circuits have upheld supervision conditions that ban Internet use altogether.[15] Others, including the Second Circuit, have favored monitoring over an outright ban, which they see as "a greater deprivation . . . than is reasonably necessary."[16] However, as the discussion above indicates, computer

personnel, *id.*, probation officers, Griffin v. Wisconsin, 483 U.S. 868, 873 (1987), and government employers, O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

[10] *Griffin*, 483 U.S. at 873.

[11] *T.L.O.*, 469 U.S. at 351 (Blackmun, J., concurring in judgment).

[12] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989).

[13] United States v. Lifshitz, 369 F.3d 173, 193 (2d Cir. 2004).

[14] Brian W. McKay, Student Work, *Guardrails on the Information Superhighway: Supervising Computer Use of the Adjudicated Sex Offender*, 106 W. VA. L. REV. 203, 220 (2003); *see also*, Ken Strutin, *Bans on Internet Use as Punishment Are Under Scrutiny*, N.Y. L.J., Jan. 11, 2005, at 5 (noting "the meaning of reasonableness in the context of restrictions on Internet or computer access is the question now facing courts").

[15] United States v. Zinn, 321 F.3d 1084, 1093 (11th Cir. 2003) (upholding a condition that required the defendant to obtain permission of the probation officer prior to accessing the Internet); United States v. Paul, 24 F.3d 155, 169–70 (5th Cir. 2001) (upholding a complete ban on Internet use as a term of supervised release for a convicted sex offender).

[16] United States v. Sofsky, 287 F.3d 122, 126 (2d Cir. 2002) (striking a condition prohibiting a probationer convicted of receiving child pornography from accessing a computer or the Internet without his probation officer's approval); *see also* Christopher Wiest, Comment and Casenote, *The Netsurfing Split: Restriction Imposed on Internet and Computer Usage by Those Convicted of a Crime Involving a Computer*, 72 U. CIN. L. REV. 847, 850–61 (2003) (providing a detailed summary of the circuit courts' treatment of Internet prohibitions).

monitoring poses its own constitutional conundrum, as it forces courts to balance individual privacy and public safety. The *Lifshitz* opinion is significant not only because it offers an approach to meeting this challenge, but also because of its broader implications for computer privacy in general.

This Comment discusses how the Second Circuit applied the special needs standard to suspicionless probationary computer monitoring and examines the possible privacy implications of its decision. Part II summarizes the facts in *Lifshitz* and the procedural background to the Second Circuit opinion. Part III presents the development of special needs jurisprudence leading up to *Lifshitz*. Part IV discusses the Second Circuit's application of the special needs doctrine in its *Lifshitz* decision. Finally, Part V considers the practical implications of *Lifshitz* along with its broader privacy implications.

II. FACTUAL AND PROCEDURAL BACKGROUND

On February 8, 2001, Federal Bureau of Investigation agents paid a visit to the home Brandon Lifshitz shared with his mother, sister and niece.[17] The agents made the house call to investigate online exchanges of child pornography on accounts registered in the name of Lifshitz's mother.[18] During an interview with the agents, Brandon admitted that he had downloaded and disseminated child pornography.[19] In addition, the family consented to a search of their computer, which uncovered pornographic pictures of children.[20] As a result, Brandon was indicted on two counts for violating section 2252A of the United States Code, which makes it a crime to knowingly receive or distribute any child pornography that has been transported in interstate commerce.[21]

Lifshitz entered a plea bargain in which he pled guilty to receiving child pornography in exchange for the state's agreement to drop the other count (for distribution).[22] During the sentencing phase, the court reviewed psychological reports that, though not in

[17] *Lifshitz*, 369 F.3d at 175.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] 18 U.S.C.S. § 2252A (LexisNexis 2004).

[22] *Lifshitz*, 369 F.3d at 176.

agreement on the precise diagnosis, all concluded that he was emotionally troubled.[23] In addition, a fourth report suggested that imprisonment could exacerbate Lifshitz's psychological problems.[24] As a result, the trial court sentenced Lifshitz to three years probation.[25]

The court imposed mandatory computer monitoring as a condition of Lifshitz's probation.[26] The terms of the condition originally required that Lifshitz consent to the installation of systems that would have enabled the probation office to monitor and filter computer use on a regular or random basis on any computer he owned or controlled.[27] In addition, he had to agree to "unannounced examinations of any computer equipment [he] owned or controlled . . . which may result in the retrieval and copying of all data from the computer and any internal or external peripherals and may involve removal of such equipment for the purpose of conducting a more thorough investigation."[28]

Lifshitz's attorney fought the search condition, citing *Griffin v. Wisconsin*[29] for the proposition that a probation officer could not conduct a search without reasonable suspicion of wrongdoing.[30] The state countered that because Lifshitz used a computer to commit his crime, the government could subject his computer to a suspicionless

[23] One diagnosed Lifshitz as suffering from a personality disorder but found no evidence that he was a sexual predator. *Id.* Another agreed that Lifshitz had a personality disorder but "provisionally diagnosed pedophilia . . . and sexual sadism." *Id.* The third doctor asserted that Lifshitz suffered from depression and obsessive-compulsive disorder at the time of his arrest, brought on by the death of his father four years earlier. *Id.* In addition, there was evidence that Lifshitz, who was thirty when he was arrested, had initiated an incestuous relationship with his sister as a teenager and had corresponded online with an 18-year-old woman to whom he paid a visit. *Id.* at 175–76. The question of whether Lifshitz was a sexual predator is relevant because the viability of conditions on Internet access depends in part on the "nexus between the crime and continued access to the Internet." Susan S. Kreston, *Computer Search and Seizure Issues in Internet Crimes Against Children Cases*, 30 RUTGERS COMPUTER & TECH. L.J. 327, 364 (2004).

[24] *Lifshitz*, 369 F.3d at 177.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] 483 U.S. 868 (1987).

[30] *Lifshitz*, 369 F.3d at 177.

search.[31] The district court agreed in part with defense counsel and inserted the words "upon reasonable suspicion" before the second part of the condition, which allowed for unannounced in-person computer searches or seizure and examination of computer equipment.[32] However, the court then held that the first part of the condition, which permitted a probation officer "to monitor and filter computer use," did not require suspicion.[33] As a result, while a probation officer could not go to Lifshitz's home to search his computer unless a reasonable suspicion prompted him to do so, an officer could remotely "monitor" Lifshitz's computer use absent any suspicion. Defense counsel appealed.[34]

III. REASONABLE EXPECTATIONS AND SPECIAL NEEDS: LEADING UP TO THE *LIFSHITZ* DECISION

A. *Creating a Foundation for Special Needs:* Camara *and* Katz

The Fourth Amendment not only guarantees the right of every person to be free from unreasonable searches, it also provides that "no Warrants shall issue, but upon probable cause."[35] There has been considerable debate over whether the Warrant Clause defines the requirements for a reasonable search or if it operates independently of the Reasonableness Clause.[36] The Supreme Court answered this question to some extent[37] in *Camara v. Municipal Court of San Francisco*,[38] when it replaced "probable cause"[39] with

[31] *Id.*

[32] *Id.*

[33] *Id.* at 177–178.

[34] *Id.* at 177.

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

[36] Jennifer Y. Buffaloe, *Special Needs and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule*, 32 HARV. C.R-C.L. L. REV. 529, 529 (1997) (stating "[a] small forest has been pulped by legal scholars" debating this issue).

[37] Christopher Mebane, Note, *Rediscovering the Foundation of the Special Needs Exception to the Fourth Amendment in* Ferguson v. City of Charleston, 40 HOUS. L. REV. 177, 188 (2003).

[38] 387 U.S. 523, 535 (1967).

[39] Probable cause requires that facts and circumstances "within the affiant's knowledge, and of which he has reasonably trustworthy information, are sufficient unto themselves to warrant a man of reasonable caution to believe that an offense has been or is being committed." Berger v. New York, 388 U.S. 41, 55 (1967) (citations omitted).

"reasonableness" as the standard of review for administrative searches, such as health and safety inspections.[40]

In the same year it decided *Camara*, the Supreme Court issued its opinion in *Katz v. United States*,[41] which declared, "the Fourth Amendment protects people, not places."[42] *Katz* is significant because it marks the Court's departure from defining Fourth Amendment protection in terms of physical spaces.[43] At the same time, the Court provided "no guidance for determining . . . *when* the Amendment protects people."[44] In his concurrence, Justice Harlan asserted that the Fourth Amendment protects an "actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[45] This expectation is crucial because if an individual does not possess it, the Fourth Amendment does not offer any protection.[46] At the same time, "Katz's malleability . . . made it especially vulnerable in cases involving technological change."[47]

The Court's new focus on individual expectations of privacy in *Katz*, and its incremental shift away from probable cause to a reasonableness standard in *Camara*, set the stage for its special needs jurisprudence.[48] Courts determine the reasonableness of a special

[40] *Camera*, 387 U.S. at 535. However, that same year, in *Berger v. State of New York*, the Court vigorously upheld probable cause as the standard for law enforcement searches. 388 U.S. 41, 57–59 (1967). In *Berger*, the Court struck a New York statute that allowed a court to issue a wire-tapping warrant upon a showing of "reasonable ground to believe" a crime had been committed because it failed to require particularity in the warrant regarding the specific crime or the "persons to be searched." *Id.* at 55–56.

[41] 389 U.S. 347, 351 (1967).

[42] *Id.*

[43] Tracey Maclin, Katz, Kyllo *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 61–62 (2002).

[44] *Id.* at 74 (emphasis added).

[45] *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Harlan's concurrence endured to become the standard today. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy or Security?*, 33 WAKE FOREST L. REV. 307, 318 (1998).

[46] Hudson v. Palmer, 468 U.S. 517, 526 (1984) (holding that the Fourth Amendment does not apply to subjective expectations of privacy that "society is not prepared to recognize as legitimate"); *Katz*, 389 U.S. at 351 (stating, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

[47] Maclin, *supra* note 43, at 75.

[48] Mebane, *supra* note 37, at 189. *Cf.* Buffaloe, *supra* note 36, at 535 (stating that *Camara* does not advance the idea that civil searches do not

needs search by balancing an individual's privacy interest against the government's need to conduct a warrantless search.[49] The Court applied this balancing inquiry in *New Jersey v. T.L.O.*,[50] which commentators point to as the Court's seminal special needs case.[51]

B. Creating the Special Needs Exception: New Jersey v. T.L.O.

In *New Jersey v. T.L.O.*, the Court examined whether the Fourth Amendment prohibited a school official from conducting a warrantless search of a student's purse upon reasonable suspicion of wrongdoing.[52] After finding that the Fourth Amendment applied to the actions of public school personnel,[53] the Court went on to state that students have an expectation of privacy in the personal items they bring with them to school.[54] However, the Court also found that the Fourth Amendment's prohibition on searches absent a warrant or probable cause would interfere with school officials' need for "swift and informal . . . procedures" to maintain discipline.[55]

A warrant requires a formal judicial proceeding, something certain to hinder school officials in their efforts to maintain discipline. Similarly, probable cause requires circumstances sufficient to believe that an offense has been committed, which may place a burden on school officials to ascertain sufficient facts prior to conducting a search.[56] On the other hand, reasonable suspicion can arise from less information or where information is less reliable.[57] The Court in *New Jersey v. T.L.O.* felt the government's interest in

require a warrant).

[49] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665–66 (1989).

[50] 469 U.S. 325 (1985).

[51] Buffaloe, *supra* note 36, at 536; Mebane, *supra* note 37, at 189.

[52] 469 U.S. at 341.

[53] *Id.* at 333.

[54] *Id.* at 339.

[55] *Id.* at 340.

[56] *See* Berger v. New York, 388 U.S. 41, 55 (1967).

[57] The Court in Alabama v. White, 496 U.S. 325 (1990), stated, "Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause." *Id.* at 330.

school discipline sufficiently outweighed students' individual privacy interests such that the lesser reasonable suspicion standard applied.[58]

The Supreme Court noted that determining the reasonableness of a search requires "a twofold inquiry . . . ."[59] It instructed courts to consider whether a search "was justified at its inception" and "reasonably related in scope" to that justification.[60] The Court declined to consider whether individualized suspicion was an essential element of the standard.[61]

The Supreme Court has not yet answered whether probationary searches require reasonable suspicion.[62] However, the Supreme Court has upheld suspicionless special needs searches outside the probation context.[63] In addition, several circuits have upheld suspicionless searches of probationers, including drug testing[64] and DNA collection.[65] Moreover, courts have noted that individuals on supervised release have lesser expectations of privacy.[66]

IV. SPECIAL NEEDS APPLIED: THE SECOND CIRCUIT'S DECISION IN *LIFSHITZ*

In *Lifshitz*, the Second Circuit chose a middle course between requiring reasonable suspicion and giving the government complete freedom to monitor a probationer's computer use. It rejected defense counsel's position that the government could not search Lifshitz's computer use without some reasonable suspicion of wrongdoing.[67] At the same time, the court did not find that the imposition of a

[58] *T.L.O.*, 469 U.S. at 340–41.

[59] *Id.* at 341.

[60] *Id.* (quoting Terry v. Ohio, 329 U.S. 1, 20 (1968)).

[61] *Id.* at 342.

[62] McKay, *supra* note 14, at 215–16.

[63] Bd. of Educ. v. Earls, 536 U.S. 822, 842 (2002) (upholding suspicionless drug testing of high school students participating in extracurricular activities); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 676 (1989) (upholding random employee drug testing).

[64] United States v. Wright, 86 F.3d 64 (5th Cir. 1996).

[65] *See, e.g.*, Roe v. Marcotte, 193 F.3d 72 (2d Cir. 1999); Boling v. Romer, 101 F.3d 1336 (10th Cir. 1996); Jones v. Murray, 962 F.2d 302 (4th Cir. 1992).

[66] *Wright*, 86 F.3d at 65 ("Persons on supervision do not enjoy absolute liberty but only conditional liberty dependent upon observance of special conditions.").

[67] United States v. Lifshitz, 369 F.3d 173, 188 (2d Cir. 2004).

search condition eliminated a probationer's expectation of privacy altogether.[68] Instead, the Second Circuit held that the special needs of the probation system were sufficient to justify suspicionless computer monitoring, but that monitoring could not be overbroad.[69] Thus, it vacated the district court ruling and remanded the case so that the lower court could ensure that the form of monitoring employed by the state bore a "'close and substantial relation' to the government's interest in pursuing the search."[70]

A. Probationary Searches and the Government's Special Needs

The Second Circuit began its analysis in *Lifshitz* by reviewing the Supreme Court's rulings on probationary searches.[71] The Supreme Court provides three reasons supporting the government's need to conduct warrantless searches in the probation context. First, community supervision aims to promote the rehabilitation of the probationer and to protect the community until the probationer achieves that goal.[72] Second, a warrant would make it difficult for probation officers to respond quickly to misconduct.[73] Finally, such a delay would dampen the deterrent effect of the search condition.[74]

In *Lifshitz*, the Second Circuit found that these special needs were particularly important in light of the government's interest in stopping child pornography.[75] Because Lifshitz used a computer to commit his crime, computer monitoring "would serve a substantial deterrent purpose."[76] As a result, monitoring would also aid in Lifshitz's rehabilitation by forcing him to keep his computer habits under control.[77] Finally, the court noted that the high rate of recidivism among sex offenders made the government's interest in

[68] *Id.* at 190.

[69] *Id.* at 193.

[70] *Id.* at 192 (quoting Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 676 (1989)).

[71] *Id.* at 179.

[72] Griffin v. Wisconsin, 483 U.S. 868, 875 (1987).

[73] *Id.* at 876.

[74] "The probationer would be assured that so long as his illegal . . . activities were sufficiently concealed as to give rise to no more than a reasonable suspicion, they would go undetected and uncorrected." *Id.* at 878.

[75] *Lifshitz*, 369 F.3d at 189.

[76] *Id.*

[77] *Id.*

deterrence and rehabilitation especially acute.[78]

B. Probationers' Reasonable Expectation of Privacy

The Second Circuit asserted that the imposition of a probationary search condition reduces a probationer's expectation of privacy.[79] The court further suggested that although individuals possess a reasonable expectation of privacy in their home computers, that same privacy interest does not extend to transmissions over the Internet or to email that has already reached its recipient.[80] In addition, the court noted that employees have no privacy interest in downloaded Internet files when their employer has implemented a policy that online activity would be monitored.[81] Thus, a probationer's privacy interests depend "on the type of monitoring implemented—whether investigating local computer activity or materials sent through an Internet Service Provider to another machine."[82]

C. Balancing Public Needs and Personal Privacy: Defining the Proper Scope of Warrantless Computer Monitoring

While the Second Circuit determined there were special needs sufficient to justify warrantless computer monitoring and a diminished expectation of privacy on the part of the probationer, the court still had to answer whether reasonable suspicion should be required.[83] As noted, the Supreme Court has not yet ruled on whether probation officers can conduct suspicionless searches of their wards.[84] Likewise, the Court has not indicated whether a

[78] *Id.* at 189–90.

[79] *Id.* at 190.

[80] *Id.* The court cited *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001), which held that individuals lack an expectation of privacy in: e-mails once they were sent to the recipient; computer records intended for public posting; and subscriber information transmitted to systems operators. *Lifshitz*, 369 F.3d at 190 (citing *Guest*, 255 F.3d at 333, 336).

[81] *Lifshitz* at 187.

[82] *Id.* at 190.

[83] *Id.*

[84] McKay, *supra* note 14, at 217. In *Griffin v. Wisconsin*, the Court held that a search of a probationer's home was reasonable because it was conducted pursuant to a valid state regulation. 483 U.S. 868, 880 (1987). The Court declined to review whether there was reasonable suspicion sufficient to justify the search at issue in the case. *Id.* at n.6. Likewise, in *United States v.*

probationer's acceptance of a search term constitutes a consent to search.[85] As a result, the Second Circuit turned to its own jurisprudence for answers.

Prior to its *Lifshitz* decision, in *United States v. Sofsky*,[86] the Second Circuit suggested that unannounced computer inspections are a preferable alternative to banning a person convicted of receiving child pornography from using a computer or the Internet absent permission from a probation officer.[87] However, the court did not reach whether reasonable suspicion should be required prior to such a search. The court's prior opinions on probationary searches did not directly address the issue either.[88] Thus, the Second Circuit looked to special needs jurisprudence in other contexts.

Without direct case law on the issue, the parties in *Lifshitz* argued over the appropriate Fourth Amendment analogy.[89] The

Knights, the Court did not reach the issue because it found that the probation officers had reasonable suspicion prior to conducting the search. 534 U.S. 112, 120 n.6 (2001).

[85] McKay, *supra* note 14, at 215. In *Knights*, the Court declined to reach the issue of whether acceptance of a search condition constitutes consent to a search because the search was reasonable under general Fourth Amendment principles. 534 U.S. at 118.

[86] 287 F.3d 122, 126 (2d Cir. 2002).

[87] *Id.* ("Although the condition prohibiting Sofsky from accessing a computer or the Internet without his probation officer's approval is reasonably related to the purposes of his sentencing . . . we hold that the condition inflicts a greater deprivation on Sofsky's liberty than is reasonably necessary.").

[88] In *United States v. Grimes*, the Second Circuit upheld a search of a parolee because the conduct of the parole officer was rationally related to the performance of her duty. 225 F.3d 254, 259 (2d Cir. 2000). The Second Circuit got closer to the issue in *United States v. Reyes*, 283 F.3d 446 (2d Cir. 2002). There, the court held that probation officers conducting a home visit do not have to have a reasonable suspicion of wrongdoing before making a home visit because probationers have a diminished expectation of privacy and home visits are not the same as a search of the home. *Id.* at 462. In *Roe v. Marcotte*, 193 F.3d 72, (2d Cir. 1999), the court upheld obtaining DNA samples from imprisoned sex offenders because the intrusion on privacy was minimal and the "lack of discretionary application of the procedure minimized the concerns traditionally underlying the requirements of probable cause and reasonable suspicion." *Lifshitz*, 369 F.3d at 187 (citing *Marcotte*, 193 F.3d at 79–80).

[89] *Lifshitz*, 369 F.3d at 182. The Second Circuit's search for an analogy is not that unusual. Analogies to "earlier notions of privacy are abundant in recent case law regarding computer technology." Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OLKA. L. REV. 99, 113 (2000).

prosecution asserted that computer monitoring is like random drug testing, which the Supreme Court has approved under certain conditions.[90] Defense counsel countered that computer monitoring, unlike drug testing, can be continuous and potentially unlimited in scope.[91] Neither side won. Ultimately, the court did analogize to drug testing, but it did so in a way that addressed the concerns expressed by the defense.

The Second Circuit's analysis honed in on those aspects of random drug testing that led the Supreme Court to decide that it did not violate the Fourth Amendment. In order to avoid a Fourth Amendment violation, the state must conduct random drug tests in a manner that is minimally physically invasive.[92] In other words, the manner in which the urine is collected should afford the individual some privacy during the act of producing the sample.[93] In addition, the test must exclude extraneous information, such as whether the person has a medical condition or eats a particular food.[94]

The Second Circuit's recommended guidelines for warrantless computer monitoring borrowed from the drug testing guidelines. Drawing on the minimally physically invasive requirement, the court focused on the method of computer monitoring. It noted that "continuous but narrowly circumscribed monitoring via software might present less of an intrusion in Lifshitz's privacy than computer searches by the probation officer."[95] In addition, the Second Circuit further instructed the district court to consider imposing filtering software if it appeared to be no less effective than continuous monitoring.[96]

The Second Circuit also focused on the fact that the Supreme Court drug testing cases required that urinalysis be "precisely targeted" to detect only drug use.[97] The court likewise required that the computer monitoring "not sweep so broadly as to draw a wide

[90] *Lifshitz*, 369 F.3d at 182

[91] *Id.*

[92] *See* Bd. of Educ. v. Earls, 536 U.S. 822, 832–33 (2002).

[93] *Id.*

[94] *Id.* at 826.

[95] *Lifshitz*, 369 F.3d at 192.

[96] *Id.* at 193. Unlike monitoring software, which continuously runs on the computer, filtering software merely blocks the user from accessing certain web pages or other online content. *Id.* at 191–92.

[97] *Id.* at 190.

swath of extraneous material into its net."[98] It noted that software designed to alert a probation officer when Lifshitz engaged in impermissible Internet activities "would bear [a] much greater resemblance to screening a probationer's urine for particular drugs—as opposed to investigating a sample to ascertain all medical conditions . . . the individual suffer[s] [from] or to figure out his or her favorite foods."[99]

By drawing this analogy, the court seemed to suggest that the state should employ computer monitoring techniques that look for illegal behavior and nothing more. Because the record before it did not reveal what kind of monitoring the probation condition authorized, the Second Circuit remanded to the district court to impose a condition consistent with its decision.[100]

Finally, the Second Circuit placed one last check on the state's power to monitor Lifshitz's computer use. It noted that in the future, Lifshitz could present evidence to the district court that equally effective, less intrusive methods of controlling his computer use were available.[101] If he made his case, the district court could modify its order accordingly.[102]

V. CONTEXT AND CONTENT MATTER: ANALYSIS AND IMPLICATIONS OF THE SECOND CIRCUIT'S DECISION IN *LIFSHITZ*

In *Lifshitz*, the Second Circuit focused on the terms of the search condition rather than on the computer as a medium. It correctly noted that a computer's versatility made it important for the court to scrutinize the nature of the search at issue.

> [C]omputers serve a multiplicity of functions, from mailbox (in sending and receiving e-mail), to telephone (in accessing particular IP addresses and web pages), to financial systems (by both permitting on-line payment mechanisms and recording personal financial data), to home offices, to storage bins. It is, therefore, not the nature of computers themselves that determines what type of search occurs, but the manner in which particular monitoring software or

[98] *Id.*

[99] *Id.* at 192.

[100] *Id.* at 193.

[101] *Id.*

[102] *Id.*

> techniques operate and the kind of computer activity that they target.[103]

Thus, the court focused on the government interest in conducting the search and the type of search rather than on whether an individual has a reasonable expectation of privacy in a computer per se.

The court's nuanced approach to computer searches prompts practical concerns as well as broader privacy implications. On the practical level, the Second Circuit's requirements that computer monitoring be minimally invasive and narrowly tailored place a substantial fact-finding burden on district courts. In terms of policy, privacy advocates may be dismayed by further expansion of the special needs doctrine and the court's apparent willingness to disregard online privacy.

A. Practical Consequences: District Courts as Technology Pundits

In the *Lifshitz* ruling, the Second Circuit left it to the district court to determine just what methods of computer monitoring are permissible. This places a heavy burden on the lower courts to review search technologies and find facts regarding their effectiveness in targeting specific types of computer use. *Lifshitz* exacerbates this burden by providing that a probationer could return to the court and request a modification of the supervision conditions upon introduction of a new privacy-enhancing search capability. In addition, each approach to computer monitoring can be circumvented depending on the technical skills of the probationer. As a result, courts must continually revise search approaches depending on the available technology and the characteristics of the probationer.

1. Finding the Right Program: Which Method is Least Intrusive but Most Effective?

The Second Circuit noted that a special needs search regime "must seek a minimum of intrusiveness coupled with maximal effectiveness."[104] But this ideal is difficult to apply in the case of computer monitoring. Courts must consider how computer monitoring software will capture and store information, what

[103] *Id.* at 183.
[104] *Id.* at 186.

information it will capture, how frequently it will collect data, and whether it may be easily circumvented.[105] A brief survey of the available monitoring technology suggests which of the available software options comply completely with the guidelines set forth in *Lifshitz*.

There are basically three types of computer surveillance software available. The first is forensic software, which essentially creates a duplicate image of the subject's computer and then systematically examines its contents.[106] The second is monitoring software, which routinely records computer activity.[107] The third is filtering or blocking software, which prevents the subject from accessing particular sites or content.[108]

a. Forensic software

Forensic software offers the most thorough, but also the most intrusive, form of computer search. Most forensic software allows the officer to create a duplicate image of a computer drive, including deleted files and unallocated data.[109] Because it can take hours to copy a single drive, it generally requires seizure of the computer to accommodate the duplication.[110] After a copy of the drive is obtained, the investigator then systematically examines its con-

[105] *See* Lanny L. Newville, *Computer Searches and Access to Monitoring Tools: A Briefing for Judicial Officers* (Jan. 4, 2002), *at* http://www.cybercrime.flmp.uscourts.gov/Presentation/CAMT.ppt.

[106] Jim Tanner, *Rethinking Computer Management of Sex Offenders Under Community Supervision*, 15 J. OFFENDER MONITORING 11 (Summer/Fall 2002), *available at* http://www.kbsolutions.com/rcm.pdf.

[107] Brian J. Kelly, *Supervising the Cyber Criminal*, 65 FED. PROBATION 8, 10 (2001), *available at* www.uscourts.gov/fedprob/2001septfp.pdf.

[108] Mark Sherman, *Introduction to Cyber Crime*, SPECIAL NEEDS OFFENDERS BULL., Aug. 2000, at 11 (noting that some districts have required filtering software as a special condition) *available at* http://www.fjc.gov/public/pdf.nsf/lookup/SNOBull5.pdf/$file/SNOBull5.pdf.

[109] Some of the more popular programs include: EnCase, Forensic Tool Kit, Professional P3, Omniquad Detective and Net Analysis. Tanner, *supra* note 106. For a discussion of the capabilities of the EnCase, Professional P3 and ComputerCop software programs, see Mark Sherman, *Cyber Crime and Cyber Terrorism*, SPECIAL NEEDS OFFENDERS BULL., Apr. 2002, at 9–10, *available at* http://www.fjc.gov/public/pdf.nsf/lookup/SNOCyb02.pdf/$file/SNOCyb02.pdf.

[110] Tanner, *supra* note 106. For a brief discussion of the legality of off-site computer searches, see Kreston, *supra* note 23, at 346–47.

tents.[111] Because this approach requires seizure of the computer and examination of every part of the drive, it falls well outside the guidelines set forth in *Lifshitz*.

Other forensics software applications are less intrusive. Some include a preview function that allows an initial search of a target drive.[112] Others run from a CD on the probationer's computer and can be set to target keywords created by the officer or selected from a predetermined list.[113] Thus, these applications can be more narrowly tailored to search for specific illegal activity and are closer to meeting the *Lifshitz* guidelines. However, these methods still require the physical presence of a probation officer in the probationer's home, a method the *Lifshitz* court described as more intrusive than continuous, narrowly tailored monitoring.[114]

b. Monitoring software

Computer monitoring software runs on an offender's machine and routinely captures information on computer activity.[115] It may do this either by capturing and saving screen images of what is displayed on the monitor or by collecting and storing keystroke data—or a combination of both.[116] Software packages may be active or passive.[117] Active programs email the results to the probation officer while passive programs store results on the probationer's computer. Because active programs do not require an in-person visit from a probation officer to retrieve information, they are less intrusive and therefore more in line with *Lifshitz* guidelines.

Most monitoring software can be used to collect everything a probationer does on his computer, including email exchanges, chat room participation, Internet activity and every keystroke typed.[118]

[111] Tanner, *supra* note 106.

[112] Sherman, *supra* note 109, at 9.

[113] *Id.* at 9–10; Kelly, *supra* note 107, at 8.

[114] United States v. Lifshitz, 369 F.3d 173, 192 (2d Cir. 2004).

[115] Some of the more popular monitoring programs include: Spector Professional, E-Blaster, STARR, Winwhatwhere, Redhand Lite and Desktop Surveillance. Tanner, *supra* note 106. For a discussion of the capabilities of the Spector, E-Blaster and Echo software programs, see Sherman, *supra* note 109, at 8–9.

[116] Newville, *supra* note 105.

[117] *Id.*

[118] Tanner, *supra* note 106.

This kind of monitoring may be too broad to comply with *Lifshitz*. The Second Circuit noted that such "constant inspection" is more like searching a diary than like a targeted drug test.[119] However, some programs include keyword triggers, which email results to the probation officer when the user has entered in specific words or phrases.[120] If the state employs this functionality, the search becomes more narrowly tailored. Thus, because computer monitoring does not require a home visit to collect the data and can be narrowly tailored, it may fall within *Lifshitz* guidelines if it is used in that manner.

c. *Filtering software*

Filtering software works either on the local user's machine or through an Internet Service Provider (ISP) or other off-site server to block access to a predefined list of sites that can be supplemented by the probation officer.[121] Others block access to sites based on a rating system.[122] This software is minimally intrusive in that it does not continuously monitor computer use. It simply blocks access to prohibited sites. On the other hand, drawbacks in the effectiveness of some programs make them undesirable as the sole means of supervision.

Filtering software that relies on lists of prohibited sites and runs on a user's computer is not an effective choice for supervision. An estimated 18 to 25 million pages of sexually related content currently exists on the Internet as well as over 700 newsgroups whose titles indicate sexual content.[123] As new Web sites crop up, probation officers face the near impossible task of updating the directory of forbidden web pages to prevent access to new content.[124] Moreover, this type of filtering would not prevent an offender from using email to send or receive forbidden materials.[125] Finally, this filtering

[119] *Lifshitz*, 369 F.3d at 191–92.

[120] For example, SpectorSoft and E-Blaster can be set to send alerts when a keyword or phrase is detected. Laura Delaney, *Monitoring Software*, PC MAGAZINE, Aug. 3, 2004, *available at* http://www.pcmag.com/article2/0,1759,1619367,00.asp.

[121] Newville, *supra* note 105.

[122] *Id.*

[123] Tanner, *supra* note 106.

[124] *See* McKay, *supra* note 14, at 235.

[125] *Id.*

software is relatively easy to circumvent.[126]

Programs that run on an ISP or other web proxy server may be more effective. A proxy server receives all file requests from a local user, retreives those requests from a different server, then relays the files back to the user.[127] It is, essentially, a middle man between the local user and the Internet. Since it can control all network traffic, this kind of filtering can be set to block inappropriate web page content as well as email messages.[128] The *Lifshitz* court provided one example of how this kind of monitoring might work in the probation context.[129] It noted a program in Bexar County, Texas, that requires probationers to use a specific ISP, which in turn keeps tabs on their online activities and denies access to sex-related sites and newsgroups or chat rooms children might visit.[130]

Because filtering software has different capabilities depending on the program used and whether it runs locally or through another server, it is difficult to make a sweeping judgment as to its suitability under the *Lifshitz* opinion. Moreover, as noted below, the effectiveness of any software depends on both the skill of the probation officer and the acumen of the probationer. Courts must weigh all these considerations when selecting a monitoring regimen for a particular probationer.

d. Circumvention issues

It is difficult to find a computer surveillance approach that is both minimally invasive and maximally effective. Each method of computer surveillance has vulnerabilities that cyber-savvy probationers may exploit. For example, offenders can defeat forensic tools by masking files through the use of layered images, encryption or steganography, which is the practice of hiding messages within a larger document.[131] Monitoring software designed for use on a specific operating system can be circumvented if the probationer simply boots from another system or from a

[126] Sherman, *supra* note 108, at 12.

[127] WIKIPEDIA, http://en.wikipedia.org/wiki/Web_proxy (defining "proxy server") (last visited Feb. 6, 2005).

[128] *See id.* (noting that many organizations use web proxies to enforce network use policies).

[129] United States v. Lifshitz, 369 F.3d 173, 192 (2d Cir. 2004).

[130] *Id.*

[131] Tanner, *supra* note 106.

different computer altogether.[132] Finally, as noted above, filtering software is also fairly easy to circumvent.[133] However, some of the problems with effectiveness can be addressed by crafting detailed probation conditions.

2. The Devil Is in the Details: Probation Conditions and Proper Training Can Maximize Effectiveness

Cyber-savvy offenders may have technological prowess far exceeding that of the officers assigned to supervise them.[134] Search conditions must be drafted "based on the experience and ability of the supervision staff conducting the monitoring, as well as the level of computer knowledge and skills the defendant possesses."[135] For example, courts should take care to add provisions that limit a probationer's ability to block monitoring software.[136] Other suggested conditions include requiring that the probationer possess only computer hardware or software approved by the probation officer; that the probationer be limited to a single computer at home and at work; and mandating disclosure of the probationer's computer passwords and ISP information.[137]

This discussion touches on the major issues facing courts as they draft computer search conditions to comply with Fourth Amendment concerns. Other practical concerns include training personnel and cost issues. Recognizing this challenge, the Federal Corrections and Supervision Division has undertaken efforts to provide guidance to the courts and training for court officers.[138] As resources on the issue grow, courts will face a lighter fact-finding burden. In the end, complying with the *Lifshitz* guidelines seems a small price to pay in

[132] Sherman, *supra* note 108, at 12. For example, a probationer can avoid Windows-based monitoring software by pressing F8 when the computer boots, bypassing Windows and using Web browsers available for DOS without detection. *Id.*

[133] *See* Sherman, *supra* note 108, at 12.

[134] Lanny L. Newville, *Cyber Crime and the Courts: Investigating and Supervising the Information Age Offender*, 65 FED. PROBATION 11, 13 (2001).

[135] *Id.*

[136] *Id.*

[137] Arthur L. Bowker & Gregory B. Thompson, *Computer Crime in the 21st Century and Its Effect on the Probation Officer*, 65 FED. PROBATION 18, 21 (2001).

[138] Newville, *supra* note 105.

exchange for the guarantee that the government's surveillance power does not exceed its legitimate grasp.

B. Privacy Implications: Public Needs and Reasonable Expectations

Privacy advocates criticize special needs searches as a slippery slope leading to an evisceration of the Fourth Amendment's demand for a minimum of individualized suspicion.[139] There is cause for concern when a court allows suspicionless computer monitoring. Moreover, *Lifshitz's* analysis of reasonable expectations of privacy draws a distinction between offline and online computer use that appears to disregard privacy interests in the latter. Although the particular need to prevent recidivism among sex offenders and child pornographers justifies the court's reasoning, any extension of the *Lifshitz* opinion beyond this context poses a significant threat to computer privacy.

1. Public Needs: Child Pornography as a Compelling Justification for Suspicionless Computer Monitoring

Special needs searches, which in some cases do not require even minimal suspicion, allow the government broad power to invade an individual's privacy. Although the *Lifshitz* ruling may be seen by computer privacy advocates as a setback, the particular need to monitor sex offenders' computer use justifies the Second Circuit's ruling. Moreover, this justification may distinguish *Lifshitz* from computer monitoring in other contexts.

In *Lifshitz*, the Second Circuit was correct in its determination that the high rate of recidivism among sex offenders and the government interest in eradicating child pornography made the need to monitor computer use particularly acute.[140] In 2002, the U.S. Department of Justice filed 1,199 cases involving child pornography and child exploitation statutes, a twenty-two percent increase from 2001.[141] Approximately 20,000 images of child pornography appear

[139] *See* George M. Dery, III, *Are Politicians More Deserving of Privacy than Schoolchildren? How* Chandler v. Miller *Exposed the Absurdities of Fourth Amendment "Special Needs" Balancing*, 40 ARIZ. L. REV. 73, 75 (1998) (stating that special needs jurisprudence created a slippery slope that allowed increasingly aggressive government intrusions).

[140] United States v. Lifshitz, 369 F.3d 173, 189–90 (2d Cir. 2004).

[141] *Indecent Exposure: Oversight of DOJ's Efforts to Protect*

on the Internet every week.[142] The Internet poses a challenge to effective supervision of offenders because it allows users to easily exchange and hide illegal images.[143] Finally, and most disturbingly, the Internet serves as a forum where sex offenders may validate their behavior and seek out victims.[144]

The dangers posed by offenders online cannot be contained with regular in-person supervision.[145] Police arrest roughly eighteen thousand sex offenders in the United States each year.[146] On average, sixty percent of those convicted receive probation.[147] Probation officers and local computer forensics labs do not have the time or resources to handle the volume of tasks presented by individually searching offenders' computers upon reasonable suspicion of wrongdoing.[148] In addition, monitoring software can capture computer activity that took place on removable drives or disks while in-person inspections cannot.[149]

Suspicionless computer monitoring not only addresses an important public safety concern, it also holds benefits for the individual searched. First, when courts have the choice to require effective computer supervision, they may forgo imposing a condition that requires a sex offender to get permission before using a computer or one that places an outright ban on computer or Internet use.[150] Indeed, in its decision in *Sofsky*, the Second Circuit indicated that monitoring is a preferable choice.[151] Second, suspicionless monitoring of sex offenders' and child pornographers' computer use may offer therapeutic benefits as it deters the aberrant behavior, thus preventing a relapse.[152]

In light of the unique circumstances in child pornography cases,

Pornography's Victims Before the S. Judiciary Comm., 107th Cong. (2003) (statement of John G. Malcolm, Deputy Assistant Att'y Gen., Crim. Div., United States Dep't of Justice).

[142] *Id.*

[143] McKay, *supra* note 14, at 209.

[144] *Id.* at 209–11.

[145] Tanner, *supra* note 106.

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] McKay, *supra* note 14, at 243.

[151] *See supra* Part IV.C.

[152] McKay, *supra* note 14, at 228.

privacy advocates should not be dismayed by the *Lifshitz* opinion. In *Lifshitz*, the court correctly expressed a reluctance to "ratify implausible or overbroad assertions of 'special needs'" and noted that the need involved "must not be isomorphic with law enforcement."[153] Rather, the court took pains to stress the particular need for the search in child pornography cases. This effort may cabin the opinion and avoid its application to computer monitoring in other contexts. As a result, the Second Circuit may have avoided greasing the special needs slippery slope.

2. Reasonable Expectations: Examining the Second Circuit's Distinctions

Interestingly, the Second Circuit's application of the reasonable expectation standard may have undermined privacy in some respects but arguably upheld it in others. The court acknowledged "distinctions between the levels of privacy that may be involved in disparate types of computer use."[154] These differences depend not only on how a computer is used, but also on whether a policy governs that use.

a. Online versus offline computer use

As noted above, the Second Circuit asserted that individuals possess a reasonable expectation of privacy in their home computers, but this expectation does not extend to Internet transmissions or sent email.[155] However, the case the Second Circuit cites to support this proposition applied to public online bulletin board postings. Thus, it is unclear whether the court meant that there is no reasonable expectation of privacy in any Internet transmission or whether it applies only to online postings intended for publication.[156]

[153] United States v. Lifshitz, 369 U.S. 173, 185 (2d Cir. 2004).

[154] *Id.* at 183.

[155] *Id.* at 190. Commentators contend, with some dismay, that the Supreme Court may not extend Fourth Amendment protection to e-mail because people perceive it as susceptible to interception. *See e.g.*, Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH. L. & POL'Y 135 (2003); Scott A. Sundstrom, Note, *You've Got Mail! (and the Government Knows It): Applying the Fourth Amendment to Workplace E-mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2087 (1998).

[156] The court first notes that individuals "may not . . . enjoy . . . an expectation of privacy in transmissions over the Internet . . . ." *Lifshitz*, 369 F.3d at 190. But it then goes on to quote *Guest v. Leis* stating, "Users would logically

The distinction is an important one. If the court meant that individuals have no privacy interest in any online communication, then such a failure to draw distinctions among types of Internet use has troubling privacy implications. If this approach to Internet communication were applied in other contexts, "the prospect of unregulated government monitoring" of email and online communication could chill legal online behavior.[157] For example, journalists and online political organizers may legitimately wish to avoid disclosure of personal contacts.[158] Permitting unfettered access to individuals' online activities "may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society."[159] Given the court's overall approach in the case, it is unlikely that it meant that individuals have no expectation of privacy in any Internet activity. The prospect that the opinion could potentially be cited as support for that proposition is a troubling one.

b. *At-work versus at-home computer use*

Privacy advocates will most likely be heartened that the Second Circuit did not hold that the imposition of a search condition eliminated a probationer's expectation of privacy. Rather, the Second Circuit distinguished between home-based and work-based computer activity. It noted that while employees have a reasonable expectation of privacy in their place of work,[160] that interest does not extend to computer files when their employer has instituted a search policy.[161] However, the imposition of a probation search condition

lack a legitimate expectation of privacy in the materials intended for publication or public posting." *Id.* (citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001)).

[157] Maclin, *supra* note 43, at 134.

[158] *Id.*

[159] *Id.*

[160] O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

[161] *Lifshitz*, 369 F.3d at 187. Several circuits have adopted this position. *See e.g.*, United States v. Thorn, 375 F.3d 679, 683–84 (8th Cir. 2004) (finding an employee has no reasonable expectation of privacy when government policy limits computer use to official government business); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (finding that an employer search policy for laptops destroyed employee's reasonable expectation of privacy); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (finding no expectation of online privacy when university policy reserved the

merely reduces (as opposed to eliminates) a probationer's expectation of privacy.[162]

Thus, even in the presence of a compelling government interest to stop child pornography, the court upheld one aspect of computer privacy by suggesting that probationers retain a privacy interest in their at-home computer use.

VI. CONCLUSION

Legal scholars express concern over the reasonable expectation approach to Fourth Amendment rights because it poses a danger that people's expectation of privacy will be "driven by what the government has the technological capability to do."[163] Others note that an objective measure of computer privacy is impossible where knowledge concerning the vulnerability of Internet transmissions and computer files varies so widely.[164] There are those who believe, perhaps rightly, that as modern technology advances, individual expectations of privacy retreat.[165] Given this foment, what is most striking about the court's decision in *Lifshitz* is its belief that new technologies could protect a probationer's privacy interests as more narrowly tailored, less invasive methods of computer monitoring become available. By rejecting the notion of a computer as a medium that could or could not be searched, the court left the door open to future technological developments that may foster greater privacy protection.[166]

right to randomly audit Internet use); Leventhal v. Knapek, 266 F.3d 64, 73–74 (2d Cir. 2001) (finding that an employee had a legitimate expectation of computer privacy but noting the absence of a computer search or use policy); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no expectation of privacy when policy explicitly limited computer use to official government business).

[162] *Lifshitz*, 369 F.3d at 190.

[163] *See e.g.*, Catherine M. Barrett, *FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy*, 8 RICH. J.L. & TECH. 16, para. 22 (Spring 2002), *at* http://www.law.richmond.edu/jolt/v8i3/article16.htm.

[164] Wells, *supra* note 89, at 112.

[165] *See* Clancy, *supra* note 45, at 335.

[166] For example, in *United States v. Balon*, the court denied the defendant's challenge to the conditions of supervised release as premature because he would not be released for another three years. 384 F.3d 38, 46 (2d Cir. 2004) ("The technology that holds the key to whether the special condition in this case involves a greater deprivation of liberty than reasonably necessary is

The other remarkable aspect of the *Lifshitz* decision is its focus on the content of the search policy. The court took great pains to ensure that the government intrusion on Lifshitz's computer privacy was as limited as possible. This is significant in light of the fact that computers and the Internet are integral to the growing dissemination of child pornography. As a result, the court's decision could conceivably be used to challenge other warrantless computer searches where the government's interest is not as compelling.

"Cases evaluating the use of surveillance technologies determine the substantive level of privacy and security of society in general, not simply whether the government's investigation of a particular individual was reasonable." [167] When a court decides to allow the government to use new surveillance technologies, it expands "government power at the expense of the public's privacy."[168] It is clear from the Second Circuit's careful, principled approach in *Lifshitz* that it took this responsibility seriously.

Shauna Curphey[*]

constantly and rapidly changing.").

[167] Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1331 (2002).

[168] *Id.*

[*] J.D. Candidate, May 2006, Loyola Law School, Los Angeles; M.A. Communications, University of Washington, August 1999; B.A. Evergreen State College, May 1995. I thank the editors and staff of the Loyola Law Review for their input and assistance. My deepest gratitude goes to my family for their love, encouragement and sense of humor, all of which sustain me.