SMART DUST: JUST A SPECK GOES A LONG WAY IN THE EROSION OF FUNDAMENTAL PRIVACY RIGHTS

Rebecca Rubin*

I. INTRODUCTION

"Every technology has a dark side - deal with it."

– Kristofer J. Pister, Professor of Electrical Engineering and Computer Sciences,
UC Berkeley[1]

The very essence of a citizen's right to privacy is embedded within the Fourth Amendment of the United States Constitution.[2] Americans inherently possess the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[3] A "search" is viewed through a societal lens of reasonable privacy expectations and a "seizure" equates to a loud interference with a person's possessory interests.[4] The inescapable inference to

*J.D. Candidate, Suffolk University Law School, 2015.

[1] Kristofer J. Pister, *SMART DUST: Autonomous Sensing and Communication in a Cubic Millimeter*, *archived at* http://perma.cc/7HZU-MSYJ (providing biographical academic information and summarizing past projects and accomplishments).

[2] *See* U.S. CONST. amend. IV (protecting against unreasonable search and seizures).

[3] *Id.*

[4] *See* Lenese C. Herbert, *Challenging the (Un)Constitutionality of Governmental GPS Surveillance*, 26 CRIM. JUST. 34, 37 (Summer 2011) (defining "search" and "seizure").

privacy protection in the Fourth Amendment is scattered throughout multiple other Amendments as well, particularly in the Ninth Amendment, which explicitly addresses the protection of those basic rights "retained by the people."[5] The rapid introduction of break-through surveillance technologies tests the scope of the Fourteenth Amendment and unenumerated privacy protections, while the law simultaneously struggles to adapt to modern changes.[6] The challenge for government is to ensure that not only are privacy protections up-held, but that there is a limited risk of misuse of these technologies by law enforcement and citizens alike.[7]

While the United States has been showered in intrusive, surveillance technologies for decades with the introduction of wiretaps, night-vision goggles, thermal imaging, beepers, and biometrics, the wildly invasive "smart dust" puts these other technologies to shame as the "ultimate privacy invasion."[8] Smart dust, miniature sensors proposed to be smaller than what the naked eye can see, has the po-

---

[5] U.S. CONST. amend. IX (stating that while there are enumerated constitutional rights, people still retain other protected rights not explicitly mentioned in the Constitution). *See* U.S. CONST. amend. IV; *see also* Bert-Jaap Koops & Ronald Leenes, *"Code" and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 125 (2005) (expanding on privacy protections as a combination of the First, Third, Fourth, Fifth, Tenth, and Fourteenth Amendments of the Constitution).

[6] *See* A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 STAN. L. REV. 1461, 1539 (2000) (discussing futurist David Brin's views about the law's weak response to rapidly increasing surveillance technology); Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 386 (Summer 1997) (discussing how the law is ill-equipped to handle the balance between law enforcement and modern science technologies); Mark G. Young, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1066 (2001) (describing problems with government control on surveillance technologies and excessive use of surveillance technology by law enforcement);

[7] *See* Young, *supra* note 6, at 1069-70 (explaining transparent surveillance technologies threaten risk of misuse); *see also* Lloyd Chebaclo, *Privacy Protections Left Wanting: Looking at Doctrine and Safeguards on Law Enforcement's Use of GPS Tracking and Cell Phone Records with a Focus on Massachusetts*, 14 J. HIGH TECH. L. 120, 145 (2014) (suggesting that clearer policy and regulations are necessary to keep up with the fast-paced emergence of modern technologies).

[8] *See* Froomkin, supra note 6, at 1500 (suggesting smart dust may be the "ultimate privacy invasion"); Young, *supra* note 6, at 1024, 1032, 1035-36 (outlining multiple technologies authorized for electronic surveillance and offering both benefits and detriments).

tential to track individuals in the most detailed aspects possible as they go about their daily lives.[9] While the public is aware that surveillance technologies carry potential privacy threats, and while the smart dust inventors claim that privacy loss will likely occur with their technology, many scholars and researchers have told the American public to simply, "get over it."[10] Smart dust is an inventive component in a new nanotechnology revolution and has the potential to monitor battlefields, transportation, the environment, medical diseases and the brain, product quality, etc.[11] Yet, while privacy is not absolute, especially within the public sphere, discreet technologies like nanotechnologies run a risk of misuse where their presence is highly undetectable.[12]

---

[9] *See* Koops & Leenes, *supra* note 5, at 140 (declaring the future of technology is suitable for perfect tracking); JAMES RULE, PRIVACY IN PERIL: HOW WE ARE SACRIFICING A FUNDAMENTAL RIGHT IN EXCHANGE FOR SECURITY AND CONVENIENCE 180 (2009) (suggesting that despite public understanding that their personal information is collected in accordance with the law, that is not enough to qualm anxieties with respect to a total surveillance society).

[10] *See* Froomkin, *supra* note 6, at 1462, 1501 (proposing one specific social response to smart dust and privacy-destroying technologies); Koops & Leenes, *supra* note 5, at 139 (describing a difficult balance between enhancing privacy and destroying it); John D. Sutter, *'Smart dust' aims to monitor everything*, CNN (May 23, 2010), *archived at* http://perma.cc/4PL5-E3WR (relaying CNN interview response from Kris Pister that "more information is better information" regarding smart dust).

[11] *See* FRANK P. GRAD, TREATISE ON ENVIRONMENTAL LAW, CH. 1, § 1.09 (Matthew Bender & Co., Inc., ed. 2013) (commenting that a new industrial revolution is fostered by information technology and is converging with nanotechnology); *see also* Froomkin, *supra* note 6, at 1501 (highlighting possibilities for smart dust application among civilians and the military); Ryan Whitwam, *Smart neural dust could carry sensors deep into the human brain, send data back out*, EXTREMETECH (July 17, 2013), *archived at* http://perma.cc/ATQ4-93MT (explaining proposals of Berkeley team in their development of smart dust to study the brain).

[12] *See* Robert D. Bickel et al., *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?* 33 STETSON L. REV. 299, 300 (2003) (illustrating privacy as contextual and subjective and non-absolute); Koops & Leenes, *supra* note 5, at 122 (emphasizing that privacy is not absolute and must be reviewed in both public and private spheres); Young, *supra* note 6, at 1044-45 (warning that particularly invasive technologies susceptible to misuse must be used in only limited circumstances). The threat of national security also promotes secret intelligence-gathering which is highly invasive, and warrants broad surveillance of individuals in any setting. This broad surveillance fosters an increased risk of misuse since those under watch cannot object

This Note will attempt to argue that while smart dust has myriad social, governmental, and scientific benefits, it is just another barrier to the fundamental liberties and protections of American citizens who roam within the public sphere. I will discuss the historical legal implications of advanced surveillance technologies such as thermal imaging, beepers, and GPS, and propose that smart dust is a vast step above this plethora of assisted physical surveillance systems, entering highly intrusive territory. Ultimately, this Note will argue that the privacy and environmental risks which follow smart dust far outweigh its benefits, and that smart dust violates protections guaranteed by the Fourth Amendment and unenumerated privacy provisions.

II. HISTORY

A. Precedent Addressing the Public Sphere

Privacy rights must be dissected within both the public and private spheres to understand just how much protection we are afforded by the Constitution and ultimately by state and federal governments. In early twentieth-century case law like Hester v. United States[13], the Supreme Court affirmed a conviction for concealing distilled spirits, and held that the special protection afforded by the Fourth Amendment, that is, the right to be free from unreasonable search and seizure, did not extend to open fields.[14] When the defendants in the case threw suspected moonshine whiskey on the ground while running from law enforcement, officers were able to arrest them without a warrant because no entry into the home occurred, and evidence was obtained outdoors in an open space.[15] *Hester* relied on common law physical trespass to determine a bright-line rule for violating one's privacy rights under the Fourth Amendment, ultimately effecting that the Fourth Amendment is irrelevant when applied to open spaces.[16]

to the technologies if they are unaware of their use. *See* Young, *supra* note 6, at 1044-45 (emphasizing misuse and invisibility).

[13] *See* 265 U.S. 57 (1924).

[14] *See id.* at 57- 59 (effecting "open fields" doctrine).

[15] *See id.* at 58 (describing the events which unfolded and led to the admissibility of evidence obtained outdoors).

[16] *See* United States v. Jones, 132 S. Ct. 945, 953 (2012) (differentiating between the Fourth Amendment's protection of open fields and its protection of residences);

In Olmstead v. United States[17] the defendants were convicted for unlawfully possessing, transporting, and selling liquor during prohibition and were caught because of police wiretaps on their telephone.[18] The *Olmstead* holding echoed the out-dated ideas of common law physical trespass, repeating that a "search" only applied to tangible items, and there is no privacy surrounding telephone calls which enter the public sphere and can be easily intercepted outside of the home.[19]

In analyzing United States v. Knotts,[20] the court expanded upon the crux of *Hester* and *Olmstead* and applied a "legitimate expectations of privacy" test to determine if the Fourth Amendment was violated.[21] In *Knotts*, officers placed a chemist of a suspected methamphetamine enterprise under watch and monitored his delivery of chloroform drums to defendant Darryl Petschen.[22] Police took their surveillance further and placed a beeper in a can of chloroform with the chemical company owner's consent.[23] The officers followed Petschen's subsequent drive to a cabin owned by defendant Leroy Knotts, and they ultimately discovered the cabin was a cover for their drug laboratory.[24] The court found that the warrantless tracking of a beeper was not constitutional because the officers discovered the drug lab only after the beeper came to rest on Knotts's private proper-

Slobogin, *supra* note 6, at 389 (iterating that the Fourth Amendment is often irrelevant when considered in the context of an area outside a residence).

[17] 277 U.S. 438 (1928).

[18] *See id.* at 455-56 (describing basic facts including that Olmstead was the lead conspirator of an illegal alcohol sales business and was subsequently convicted in the Western District of Washington District Court for violation of the National Prohibition Act).

[19] *See id.* at 466 (explaining that Fourth Amendment protection does not apply to non-tangible effects).

[20] *See* 662 F.2d 515 (8th Cir.1981).

[21] *See id.* at 516-17 (describing current Fourth Amendment analysis that persons are protected against the government's unreasonable intrusions without either a warrant or probable cause because of their legitimate expectations of privacy).

[22] *See id.* at 516 (outlining visual surveillance operation of "chemist" Tristan Armstrong, a member of the methamphetamine enterprise who was indicted but testified against other enterprise members, Knotts and Petschen).

[23] *See id.* (affirming that despite success of the visual surveillance, officers switched to electronic surveillance to undercover more details of operation).

[24] *See id.* (elaborating that with the use of the electronic surveillance, law enforcement was able to encounter the delivery location of the can of chloroform , and could confidently execute warrants for a search of the cabin/drug laboratory).

ty.[25] The court admitted that even though beepers reveal what may have already been in public view, the beeper ultimately landed in a private sphere that would not normally have been accessible to the public, and therefore, Knotts had a reasonable expectation of privacy.[26] However, though Petschen tried to argue that he had a subjective expectation of privacy, the Court ruled that his argument had no weight since he passed through public thoroughfare and traveled to a property which he did not possess.[27]

While landmark constitutional privacy rights cases contain facts, which differ drastically from modern surveillance technologies, their monumental holdings lay the foundation for an individual's basic rights. Griswold v. Connecticut[28] allowed married couples to operate their fundamental right to choose contraceptives over procreation, free from government interference.[29] While *Griswold's* holding stressed that one of the most cherished events in a person's life is a person's marriage and emphasized that marriage should be protected, it addressed the broader need for personal autonomy free from government intrusions and explicitly protected Fourth Amendment privacy rights.[30] Similarly, Lawrence v. Texas[31] upheld the personal autonomy of homosexuals to engage in sexual intimacy within the private sphere of their homes, following police interference during the defendants' private act and their subsequent arrests.[32] *Lawrence*

---

[25] *See id.* at 518 (affirming violation of privacy occurred where the beeper came to rest in a private space).

[26] *See Knotts*, 662 F.2d at 518 (holding Knotts had legitimate privacy expectation where "society is prepared to recognize [intrusion on his private property] as reasonable").

[27] *See id.* (explaining that a subjective expectation of privacy was not enough to warrant a reasonable expectation of privacy).

[28] *See* 381 U.S. 479 (1965) (concluding that the right of privacy to use birth control measures was legitimate).

[29] *See id.* at 486 (emphasizing the zone of privacy established by multiple amendments and the restrictions on government when they unnecessarily invade that zone).

[30] *See id.* at 483-86 (explaining the application of privacy rights to the First, Third, Fourth, Fifth, and Ninth Amendments and safeguarding marriage as a sacred institution).

[31] *See* 539 U.S. 558 (2003).

[32] *See id.* at 562-63, 577-78 (describing the facts of how police entered the residence in response to a weapons disturbance and interrupted "deviate sexual intercourse" of petitioners, and further summarizing the ultimate holding of the case

iterated the important point that "freedom extends beyond spatial bounds," hinting that perhaps even private moments should be protected within the public sphere.[33]

B. Precedent Addressing the Private Sphere

The legitimate expectation of privacy test referenced in *Knotts* originated out of Justice Harlan's concurrence in Katz v. United States[34] where he laid out the twofold requirement that (1) a person exhibit "an actual (subjective) expectation of privacy," and (2) "that the expectation be one that society is prepared to recognize as reasonable."[35] *Katz* iterates the notion that the Fourth Amendment protects people, not places, and that what a person knowingly exposes to the public is not constitutionally protected.[36] Where the defendant entered a phone booth with the expectation that there would be no intruding ears (even in the course of transmitting wagering information in violation of a statute) his acts were protected by the Fourth Amendment because he placed a call, shut a door behind him, and society reasonably expects a public telephone booth to allow for private communications.[37] *Katz* effectively overruled *Olmstead* and

---

that there is no governmental interest which can substantially outweigh personal autonomy).

[33] *See id.* at 562 (introducing the concept of individual liberty beyond private spheres like the home).

[34] *See* 389 U.S. 347 (1967).

[35] *Id.* at 361 (Harlan, J., concurring).

[36] *See id.* at 351 (expressing that the argument of a "constitutionally protected area" does not carry as much weight as a person's overall privacy, and what is preserved as private, even within the public sphere like a phone booth, garners constitutional protection).

[37] *See id.* at 352-53 (rejecting the "trespass" doctrine where only a physical intrusion equates to an unreasonable search or privacy violations under the Fourth Amendment). *Katz* details the Court's holding in *Olmstead* when it narrowly interpreted Fourth Amendment protections under the "trespass" doctrine, deciding no physical trespass or physical seizure of information can result in a violation*; see also Olmstead*, 277 U.S. at 464-66 (suggesting the Fourth Amendment only applies to material things). *Katz* explicitly rejects that holding because electronic surveillance allows for intangible information to be recorded and seized. *See Katz*, 389 U.S. at 353 (concluding that *Olmstead* has been eroded by modern technology and the concept of justifiable reliance of a person using a phone booth for a private conversation is sufficient as a Fourth Amendment violation without the need for physical interference).

erased the out-dated doctrine that unreasonable search and seizure cannot apply to non-physical things.[38]

Following the *Katz* test implemented by Justice Harlan, Kyllo v. United States[39] posed a challenge to the Supreme Court to determine the limits of technology to "shrink the realm of guaranteed privacy."[40] *Kyllo* involved law enforcement's use of a thermal imaging device to study the heat exuding from the defendant's home in order to determine if marijuana was being grown inside.[41] The lower courts found that "no intimate details of the home were observed" removing objective privacy, and that no subjective privacy was shown on behalf of the defendant because he did not try to conceal the heat.[42] However, the Supreme Court considered that modern thermal imaging technology allowed for far more than "naked-eye surveillance," where the warrantless obtainment of information from inside a person's home intruded upon Kyllo's intrinsic privacy expectations, and hence, violated the Fourth Amendment.[43] The Court further differentiated between "off-the wall" observation and "through-the-wall" observation, concluding that heat emanating from the walls of the home led to the discovery of intimate details.[44]

In 2009, People v. Weaver[45] introduced the controversy surrounding the use of the Global-Positioning System ("GPS") to track

---

[38] *See Katz*, 389 U.S. at 353 (eliminating the trespass doctrine for good).
[39] *See* 533 U.S. 27 (2001).
[40] *See id.* at 34 (asserting the specific question posed to the Court in determining Kyllo's rights and privacy concerns).
[41] *See id.* at 30 (reiterating the efforts of law enforcement).
[42] *See id.* at 30-31 (describing holdings of District Court and Appeals Court based on reasonable expectations of privacy).
[43] *Id.* at 33-34 (discussing the Court's consideration of modern technology, its effect on the Fourth Amendment, and the overall concept that the home affords heightened privacy protection).
[44] *See id.* at 35-36 (unraveling the issue presented in Justice Stevens' dissent where the homeowner would essentially be at the "mercy of advancing technology" if the dissent's argument was valid). Justice Stevens argues that a subjective expectation of privacy for the heat inside a home is unreasonable since heat waves enter public domain the moment a door opens. *See Kyllo*, 533 U.S. at 43-44 (Stevens, J. dissenting). The majority refutes this argument concluding that all details in the home are intimate and protected. *See id.* at 37-40 (rejecting dissent and concluding that it was only because of the physical intrusion of the technology used that the intimate details were so discoverable, beyond just simple external heat waves).
[45] *See* 909 N.E.2d 1195 (2009).

potential criminals without a warrant in the state of New York.[46] Law enforcement placed a GPS under defendant's bumper and monitored him continuously for sixty-five days, leading to his eventual conviction for burglary.[47] The New York Court of Appeals reversed defendant's conviction, holding that GPS is a groundbreaking technology with the ability to monitor enhanced details of an individual's everyday life for an unlimited period, and when used incorrectly, without a warrant, the technology can clearly threaten Fourth Amendment rights.[48] While the *Weaver* court could only rule on behalf of state law, it addressed the need for resolve in federal court and characterized the manipulation of the GPS technology as a "gross intrusion" of defendant's constitutional rights and limitation of his personal freedom.[49]

Finally, in 2012, the Supreme Court analyzed law enforcement's misuse of GPS technology when a GPS was placed on the undercarriage of the defendant's Jeep without a warrant in United States v. Jones.[50] Repeating the notion that the Fourth Amendment protects people, not places, *Jones* held that this warrantless search violated the defendant's Fourth Amendment rights, especially where using GPS allowed law enforcement to physically occupy private property to obtain information.[51] The Court urged that property protections are closely linked to privacy protections, echoing the ideas of common

[46] *See id.* at 1196 (outlining premise of controversy where surveillance was conducted without a warrant).
[47] *See id.* (addressing the nonstop, warrantless surveillance of defendant Weaver using a specific device known as a "Q-ball," which used satellites to receive location data, and explaining the charges of the crime).
[48] *See id.* at 1199, 1202 (addressing GPS as a sophisticated technology with powerful tracking capability and holding that constant, warrantless GPS surveillance is a clear "search" in violation of the New York state constitution).
[49] *See id.* at 1202-03 (characterizing the constant GPS surveillance as a "gross intrusion" where law enforcement had no grounds to monitor defendant without a warrant and clarifying that the matter remains undecided in federal courts).
[50] *See* 132 S. Ct. at 949 (concluding the installation of a GPS tracker by the government constituted a search under the Fourth Amendment).
[51] *See id.* at 949 (stressing that a Fourth Amendment violation occurred through the manipulation of defendant's property, and arguing that the Framers would have left "effects" out of the amendment if they did not intend to protect it); *Katz*, 389 U.S. at 351 (affirming *Katz's* Fourth Amendment protection explanation of people, not places).

law trespass, which guaranteed a minimum degree of privacy protection.[52]

Justice Sotomayor's concurrence in *Jones* affirmed similar arguments in Justice Alito's concurrence, where both justices relied on the *Katz* test.[53] Justice Sotomayor questioned whether people should reasonably expect the government to record movements and other information, which can reveal intimate details about people's lives, using highly capable technologies such as GPS.[54] Justice Alito reveals in his concurrence that technology can change a person's reasonable expectations and thus alter the *Katz* test, and as technological advances occur, many people may welcome the loss of privacy in exchange for strengthened security measures.[55] Justice Alito provides a modernized and predictive view that the widespread availability of technologies similar to GPS may make long-term monitoring easier and cheaper, uncovering a "degree of intrusion" unanticipated by a reasonable person.[56] The rampant availability of surveillance technologies broadly addressed by Justices Sotomayor and Alito in their concurrences indicates that government regulations are necessary to undermine future fears of unreasonable privacy invasions, especially where technology is rapidly advancing.[57]

---

[52] *See Jones*, 132 S. Ct. at 953 (arguing that personal property is constitutionally protected and has been for centuries). The Court rejects the concurrence's desired and exclusive application of the *Katz* test in this case, arguing that both ideals apply here. *See id.* at 952-53 (emphasizing *Katz* is not a substitute for the common law trespassory test, but adds to it).

[53] *See id.* at 955 (Sotomayor, J., concurring) (maintaining Alito's position that physical surveillance is unnecessary for modern surveillance, and the *Katz* "legitimate expectations of privacy" test will be re-shaped through rapid technological advances).

[54] *See id.* at 956 (Sotomayor, J., concurring) (noting that surveillance technology like GPS can expose intimate details about the public).

[55] *See id.* at 962 (Alito, J., concurring) (theorizing the effects of technological advancement on the public's perceptions of their privacy rights).

[56] *See id.* at 964 (Alito, J., concurring) (warning that modern devices may result in much-needed government regulations where privacy invasions may be greater than expected by the public).

[57] *See Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring) (agreeing with Alito's contention that GPS and similar technologies allow for long-term monitoring, creating greater privacy concerns); *see also id.* at 964 (Alito, J., concurring) (predicting that modern surveillance technologies allow for longer-term monitoring which impedes upon privacy expectations, and addressing how government entities are the only able bodies to provide adequate solutions).

C. Attempts at Regulating Surveillance Technology

1. Congressional Response

Government efforts to reduce privacy intrusion by law enforcement have historically occurred through the following federal acts, which target communications. In 1934, Congress enacted the Communications Act, creating a *per se* prohibition on the interception of communications by any party, including law enforcement.[58] In 1968, Congress created Title III of the Omnibus Crime Control and Safe Streets Act which enacted a general prohibition on wiretapping, but allowed an exception for law enforcement where under certain situations, authorities could legally intercept oral, electronic, and wire communications without any consent.[59] These "certain situations" usually applied to apparent criminal activity, and the statute's application appeared in the form of a heightened search warrant, allowing for 30-day periods of surveillance upon court approval.[60]

Title III underwent multiple amendments to reflect changing telecommunications society, two changes of which included the Electronic Communications Privacy Act of 1986 ("ECPA") and the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").[61] The ECPA was enacted in response to what was then

---

[58] *See* Communications Act of 1934, 47 U.S.C. § 151 (1934) (enacting regulations for interstate or foreign communication by wire or radio and describing purpose of the act); *see also* Young, *supra* note 6, at 1057 (describing Congressional Communications Act of 1934).

[59] *See* Young, *supra* note 6, at 1057-58 (describing purpose of Title III and requirements for use, codified and amended as 18 U.S.C. §§ 2510-2522). The Omnibus Crime Control and Safe Streets Act of 1968 has 11 titles but Title III refers specifically to electronic and wireless surveillance to ensure public safety and an effective response to crime. *See* The Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (as amended 2013) (enacting regulations in response to increased crime and surveillance, and to achieve effective law enforcement).

[60] *See* Young, *supra* note 6, at 1058-59 (outlining requirements for law enforcement's use of Title III, where only high-ranking officials within the U.S. Attorney General's office can submit an application, and facts must show probable cause of the likeliness of a crime or actual commission of a crime).

[61] *See* 18 U.S.C. §§ 2510-2522 (1968) (enacting regulations to protect against unlawful surveillance and wiretapping by law enforcement); Communications Assis-

"new electronic communications" such as email and voicemail.[62] CALEA was a direct response to continue the allowance of electronic surveillance by law enforcement while requiring telecommunication carriers to allow for interceptable lines.[63] However, the interception of communications did not apply to cordless telephones.[64]

Congress has further placed limits upon the executive branch with the enactment of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), providing that the President must obtain a surveillance order to conduct wiretapping in the face of national security threats.[65] Following 9/11, the USA Patriot Act of 2001 gave law enforcement broader powers to wiretap under suspicions of terrorism.[66]

2. Non-Legal Proposals

tance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) [hereinafter CALEA] (enacting clear telecommunication carrier duties to cooperate with law enforcement in the interception of communications); *see also* SUSAN BRENNER, CYBERCRIME AND THE LAW: CHALLENGES, ISSUES, AND OUTCOMES 154 (2012) (explaining the evolution of Title III and how early acts prior to the 1980s were concerned solely with telephone calls, but changed as modern communications like email developed); Young, *supra* note 6, at 1059 (highlighting new communications laws which reflected changing society).

[62] *See* 18 U.S.C. §§ 2510-2522 (1968) (stating the law concerning cybercrimes relating to interception of oral and electronic communications); *see also* BRENNER, *supra* note 61, at 155 (expanding upon the ECPA and how the SCA was a provision of that act and intended to protect communications held in electronic storage); Young, *supra* note 6, at 1059 (stating purpose of ECPA to protect against unlawful law enforcement surveillance).

[63] *See* Young, *supra* note 6, at 1060 (stating the focus of CALEA was to regulate the interception of communications).

[64] *See* Young, *supra* note 6, at 1059-60 (identifying limitations CALEA places upon law enforcement).

[65] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (1978) [hereinafter FISA] (regulating surveillance of foreign powers involved in interstate terrorism or activity against the United States); *see also* Young, *supra* note 6, at 1060 (explaining procedures implemented through FISA and requirement for U.S. President to obtain a court order to conduct wiretapping for national security purposes).

[66] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter USA PATRIOT Act] (enacting legislation to provide adequate security measures for counterterrorism, specifically in response the 9/11 attacks); *see also* Young, *supra* note 6, at 1064 (describing USA PATRIOT Act and how the act reflects an exception for Title III wiretapping).

Aside from congressional efforts, non-legal privacy protections like self-regulation have been urged by the government.[67] Self-regulation relates to electronic data collection where consumers and electronic marketplaces alike can take preventative measures for giving out personal information to third-parties.[68]

Further, privacy-enhancing technologies ("PETs") allow consumers more privacy over the internet by limiting data collection of personal information, and these types of privacy constraints can be embedded in software and systems by systems designers.[69] Encryption is a leading PET with electronic communication and "cryptography" allows for the protection of communications and stored electronic data.[70]

Despite a history of legislation to protect citizens' privacy interests, regulations appear minimal at best and more so reflect the erosion of privacy.[71] Without congressional assistance, non-legal proposals remain largely ineffective.[72]

III. FACTS[73]

[67] *See* Froomkin, *supra* note 6, at 1524, 1527 (stating government is asking internet industry to self-regulate by disclosing privacy policies on consumer sites to ease its own burden).

[68] *See* Froomkin, *supra* note 6, at 1524-25 (defining and self-regulation and arguing government intervention is essential to enforce this type of regulation).

[69] *See* Froomkin, *supra* note 6, at 1528-29 (describing the function of PETs and the role of law in creating obstacles for PETs).

[70] *See* Froomkin, *supra* note 6, at 1530 (pointing out encryption as the major PET). However, the United States is wary of the use of encryption, since communications can easily be shielded from eyes of investigators using this PET. *See* Froomkin, *supra* note 6, at 1530 (emphasizing unattractiveness of encryption to United States government); Koops & Leenes, *supra* note 5, at 144 (defining cryptography and uses).

[71] *See* Young, *supra* note 6, at 1062 (highlighting the overall trend of legislative erosion of privacy interests).

[72] *See* Froomkin, *supra* note 6, at 1527 (warning that without legislative interference, self-regulation offers minimal privacy protection). Self-regulation requires the voluntary participation of online marketplaces and without economic incentives for participants, it is weak at best. *See* Froomkin, *supra* note 6, at 1524-27 (elaborating upon self-regulation as a weak privacy protection scheme).

[73] The author of this note would like to stress that she is by no means an expert in the field of electrical engineering and this section is intended to provide merely a brief overview of a very complex and scientifically advanced technology. She

While the world remains hungry for increasing innovative technologies, researchers at the University of California, Berkeley ("UC Berkeley") have been dreaming up an elaborate nanotechnology, miniature in size but gargantuan in scientific capabilities. The Smart Dust project, created by researcher Kris Pister in the 1990s, reflects his previously only-imagined idea of a world of constant monitoring through the use of countless tiny sensors sprinkled upon the Earth.[74] Pister, a professor of electrical engineering at UC Berkeley,[75] created smart dust, a micro-millimeter scale technology capable of both military and commercial application for sensing vibrations, temperatures, sounds, and lighting, among other elements.[76] In their 1998 memorandum, Pister and colleagues proposed smart dust as a package composed of hundreds to thousands of different types of sensors to serve as communication platforms between monitored information and a base transceiver.[77] Once a theory, smart dust is now a reality.[78] Smart dust is in the beginning stages of design, but Pister's ultimate goal is to market the technology as cheap and efficient wireless communication devices, compact in size at no larger than one cubic millimeter, or equal to a speck of dust.[79]

points readers to her cited sources in this section for a developed technical analysis of smart dust.

[74] *See* Sutter, supra note 10 (describing Pister's basic idea behind smart dust and explaining related projects and benefits).

[75] *See* Kristofer Pister, BERKELEY ELECTRIC ENG'G. & COMPUTER SCI. (Feb. 21, 2015), *archived at* http://perma.cc/45WY-F4PP (offering a brief biography of Kristopher Pister as well as a list of selected publications).

[76] *See* V.S. Hsu et al., *Wireless Communications for Smart Dust*, DEP'T OF ELEC. ENG'G & COMPUTER SCI. (Jan. 30, 1998), *archived at* http://perma.cc/MCM3-QW6Q (describing both commercial and military applications for smart dust); Kristofer S.J. Pister, *Smart Dust: BAA 97-43*, *archived at* http://perma.cc/PX3-ECS7 (outlining multiple sensor uses including specific applications in military and commercial settings).

[77] *See* Hsu et al., *supra* note 76, at 1 (explaining the goal of smart dust); J. M. Kahn et al., *Next Century Challenges: Mobile Networking for "Smart Dust,"* DEP'T OF ELEC. ENG'G & COMPUTER SCI, *archived at* http://perma.cc/FQ3G-HR87 (presenting research about smart dust technology and integration of multiple parts into a single package).

[78] *See* Sutter, *supra* note 10 (providing background on the development of Pister's smart dust technology).

[79] *See* Hsu et al., *supra* note 76, at 1 (describing small size ranging from a cubic millimeter to the size of a sugar cube and dramatically reduced costs). *See also*

Funded by the Defense Advanced Research Projects Agency ("DARPA") for approximately $2,950,000, Pister and his team are faced with a momentous challenge to successfully develop tiny motes comprised of micro-electromechanical sensors ("MEMS") which communicate with one another, are self-powered, and report to a main transceiver base in real-time.[80] The dust motes or sensor nodes are to be composed of a power supply, a specific type of sensor, such as vibration, temperature, or sound, a circuit or electrical source, and a communication element.[81] The sensors operate on a cueing system where they detect a certain element, like heat, sound, or motion, and communicate back and forth using either passive or active communications – both methods are currently being debated but passive is most favored.[82] In a passive communication set-up, a sensor alerts the others when it detects its critical event "signature," such as a heat sensor that detects a large mass of body heat distinguishing a human

Marshall Brain, *How Motes Work*, HOWSTUFFWORKS, *archived at* http://perma.cc/NH8P-53BB (providing information about smart dust technology or "mote" as a low-cost, low-power computer).

[80] *See* Kahn et al., *supra* note 77 (outlining basic challenges researchers are faced through the development of smart dust); Pister, *supra* note 76 (offering amount of DARPA funding on cover page of proposal).

[81] *See* Pister, *supra* note 76, at 2 (outlining components of smart dust motes or sensor nodes).

[82] *See* Kahn et al., *supra* note 77 (describing efficient method using a cueing system and relying on passive communication to maintain power efficiency)*; see also* Hsu et al., *supra* note 76, at 2-3 (exploring system design options but favoring free-space passive transmissions, consuming only solar power or non-battery power, over active transmissions which usually run on battery power requiring an excessive power source). This research proposal further differentiates between the benefits of using passive communication technology over active communication technology since active communication requires more power, and hence more cost. *See* Kahn et al., *supra* note 77 (summarizing the attributes of both active and passive transmissions and discussing the differences between the two). In passive communication, a device reflects a signal directly back to the source which is idle sending information one-way, whereas in active communication, devices must communicate continuously with each other causing chain communication. *See* Kahn et al., *supra* note 77 (explaining how passive communication works). Active communication is less favored for the design of smart dust because collisions with information floating freely in the air are more likely to occur, and the expense for frequent communication is greater, especially where there is more power consumption. *See* Kahn et al., *supra* note 77 (discussing why active communication is less favored than passive communication for the design of smart dust).

from a small animal.[83] This mechanism of peer-to-peer sensor communication can only work when the sensors are wildly dispersed and not in another sensor's line-of-sight.[84] Communications between sensors are proposed to last over a number of days or more, but the proper power source is key and solar power or some type of light source is most favored, especially to keep costs down.[85]

While the original proposals of smart dust were to release these dust-like particles in the air allowing them to be essentially buoyed by air currents and relaying information about the environment and people in real-time, proposals have been narrowed for specific application on military battlefields, sensing environmental hazards, and reading brainwaves.[86] The inner-workings of the application of smart dust in the military is described as a battlefield sensor network where sensor nodes are delivered by helicopter and track the motions of military vehicles to search for intruders or unsuspected activities, reporting back to a receiver via live video.[87] Essentially, sensor motes with acoustic, vibration, and magnetic field sensors can cover miles of land and report any large vehicles to the

---

[83] *See* Kahn et al., *supra* note 77 (providing example of passive communication transmission and emphasizing the use and benefits of "emergent" or swarm-like behavior of sensors); Sutter, *supra* note 10 (reaffirming initial proposal to scatter smart dust particles in the air).

[84] *See* Kahn et al., *supra* note 77 (covering line-of-sight requirement and necessity for unblocked communications and further explaining that a blocked line-of-sight requires the use of active transmissions). The urge for a radically small size, such as one cubic millimeter, will likely help to reduce any blocked line-of-sight issues. *See* Kahn et al., *supra* note 77 (explaining that the small-size of a dust mote will allow for an increase of line-of-sight during use, which is normally required for operation of free-space optical links for Smart Dust).

[85] *See* Kahn et al., *supra* note 77 (affirming the notion that a low-power source like solar power saves energy and expense).

[86] *See* Kahn et al., *supra* note 77 (exploring the realm of possibility for smart dust to be small enough to suspended in the air, buoyed by air currents); Pister, *supra* note 76, at 3 (detailing application of smart dust in battlefields); Sutter, *supra* note 10 (relaying Pister's original ideas to monitor information about people, cities, and the environment); Whitwam, *supra* note 11 (addressing proposals of smart dust for studying the human brain); *see also How Smart Dust Could Spy On Your Brain*, MIT TECH. REV. (July 16, 2013), *archived at* http://perma.cc/X5NZ-ZZTN [hereinafter MIT TECH. REV.] (providing further overview of UC Berkeley researchers' plans to use neural dust sensors for studying and interacting with the brain).

[87] *See* Pister, *supra* note 76, at 3-4 (illustrating the integration of chem and bio sensors into smart dust system for military use).

ground controller in real-time, and can further be carefully placed on aircrafts or ground vehicles versus random spatial distribution.[88]

In military application, smart dust may also be able to detect the presence of hostile biological agents or harmful chemicals on a battlefield.[89] In general, smart dust may eventually be able to detect harmful biological components in the air, not solely on battlefields, to ensure that ecosystems are healthy and to detect the possible presence of natural disasters like earthquakes.[90] Another main proposal is to implement smart dust to study and monitor weather conditions and to discover environmental toxicities.[91] Finally, there may be a use for predicting traffic patterns or monitoring parking spots (similar to a technology that has already been implemented in San Francisco), as well as aiding in oil exploration.[92]

MIT is currently exploring possible ways to use smart dust to interact with and study the human brain by sprinkling tiny electronic sensors into the cortex and using ultrasound to remotely interrogate the pulses of the sensors.[93] There are many hurdles to this approach however, and even a low-powered, portable device like smart dust poses some difficulty: the power must be low enough to avoid heating the skull and brain, and this "neural" dust must be tiny enough to overcome an implantation problem, and viable enough to last perhaps indefinitely inside the cortex.[94] Ultrasound is a feasible resolution to some of those problems where it can keep the neural network charged without overheating any necessary organs in the body.[95] Dongjin Seo,

---

[88] *See* Pister, *supra* note 76, at 4, 12 (detailing sensor type and scenario for reporting information).
[89] *See* Kahn et al., *supra* note 77 (describing particular military use of smart dust).
[90] *See* Sutter, *supra* note 10 (highlighting environmental purposes of smart dust); *see also* Kahn et al., *supra* note 77 (discussing use of smart dust to perform environmental measurements where wired sensors lead to errors).
[91] *See* GRAD, *supra* note 11 (discussing environmental advantages of smart dust).
[92] *See* Sutter, *supra* note 10 (touching upon various uses of smart dust to uncover oil locations by studying rock vibrations, covering a 6-square-mile area, and describing San Francisco's installation of 12,000 wireless sensors to determine if there is a car in a parking spot and alert others).
[93] *See* MIT TECH. REV., *supra* note 86 (discussing UC Berkeley researchers' idea to use smart dust in brain study).
[94] *See* MIT TECH. REV., *supra* note 86 (setting forth advantages to smart dust and subsequent challenges).
[95] *See* Whitwam, *supra* note 11 (discussing advantages of using ultrasound in implementation of brain studies).

one of the main researchers behind the implementation of smart dust in medical study, has explained that using wireless sensors eliminates risk of infection from wiring while providing real-time monitoring of brain functions, mirroring President Barack Obama's BRAIN initiative.[96] This wave of "micro-motes" in medical or biological use also poses body heat as another possible power source when dealing with such a small-scale design that must be powered for lengthy periods of time.[97]

The advent of smart dust follows the progression of other wired and wireless sensor technologies that have persisted for decades, such as Closed-Circuit Television ("CCTV"), Radio Frequency Identification ("RFID"), and GPS.[98] CCTV, a prevalent surveillance system in London, which was estimated to snap about 300 pictures of the average citizen a day in 2007, has merely been the beginning of the progression of other individual surveillance systems such as the

---

[96] *See* Elise Ackerman, *How Smart Dust Could Be Used To Monitor Human Thought*, FORBES (July 19, 2013), *archived at* http://perma.cc/9TQP-DX8N (relaying Seo's proposal for neural dust). Obama's BRAIN initiative, or Brain Research through Advancing Innovative Neurotechnologies, enacted in April 2013, emphasized such a need for the large-scale recording of neurons. *See also* Dongjin Seo et al., *Neural Dust: An Ultrasonic, Low Power Solution for Chronic Brain-Machine Interfaces*, DEP'T OF ELEC. ENG'G & COMPUTER SCI., (July 8, 2013), *archived at* http://perma.cc/NW2Q-2V2K (addressing the BRAIN initiative). The BRAIN Initiative is a revolutionary research effort backed by President Barack Obama to uncover new treatments for Alzheimer's, schizophrenia, autism, epilepsy and traumatic brain injury. *See Brain Initiative*, WHITE HOUSE (Sept. 30, 2014), *archived at* http://perma.cc/NE8B-VGPW (offering preliminary information regarding the BRAIN Initiative). Scientists were awarded approximately $100 million to develop research and strategies, and DARPA was given $50 million of that budget to understand dynamic brain functions. *See id*. (highlighting the various funding allocations to neuroscience research and development organizations). Goals of the BRAIN Initiative include: understanding how the brain leads to different perceptions and decision making, developing new related technologies, providing knowledge to address debilitating diseases, and studying individual genes and neurons to understand behavior. *See id*. (explaining the objectives and ambitions of the BRAIN Initiative).

[97] *See* Graham Templeton, *Smart dust: A complete computer that's smaller than a grain of sand*, EXTREMETECH (May 15, 2013), *archived at* http://perma.cc/LL7Z-BRB6 (discussing breakthrough technology crafted by University of Michigan researchers that is a highly functioning computer, less than a millimeter in size which is fitted with a tiny solar cell and has been compared to smart dust, posing same barriers like power source and overall communication methods).

[98] *See* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2324-34 (2007) (outlining multiple types of sensors which already exist in the world).

camera-phone.[99] The very visible camera-phones in almost every cell-phone user's hand will eventually "melt…further into invisibility."[100]

While camera sensors share information with people, the sensors established in RFID share information with other machines to perform a wider-range of monitoring functions.[101] The RFID characteristics mirror those of smart dust where both technologies are wireless, communicate with machines, enable advanced tracking, and are relatively cheap, making attractive devices within the marketplace.[102] RFID can be as small as a grain of rice and can track both tangible items and locations or movements.[103] RFID functions as a tagging and tracking system, where the locations and activities of individuals are revealed every time an EZ-Pass crosses through a toll booth, or a subway card is flashed at a turnstile entryway.[104] RFID has its share of benefits where it could lead to the identification of stolen property and greatly assist law enforcement in overall theft reduction.[105] However, RFID also carries a fair amount of concerns if improperly used by law enforcement to apprehend criminals.[106]

---

[99] *See id.* at 2324-26 (highlighting the prevalence of CCTV in London and the advent of personal devices like the camera-phone in contributing to lessened privacy and increased surveillance).

[100] *Id.* at 2329 (summarizing that technology is evolving and miniaturizing its components, leading to increased invisible surveillance).

[101] *See id.* at 2329-30 (comparing people-shared information with machine-shared information).

[102] *See id.* at 2330-31 (describing components and benefits of RFID).

[103] *See* Brief of the Rutherford Institute and the National Motorists Ass'n, as Amici Curiae Supporting Respondent, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 4826981, at *12 [hereinafter Brief for the Respondent] (summarizing characteristics of RFID technology).

[104] *See* Kyle Sommer, *Riding the Wave: The Uncertain Future of RFID Legislation*, 35 J. LEGIS. 48, 48 (2009) (offering examples of RFID chip presence in everyday society).

[105] *See* Joseph Christiana et al., *Law Enforcement Response to Concerns Regarding RFID Technology* (Mar. 2, 2007), *archived at* http://perma.cc/9H5H-S9T9 (presenting tagging benefits such as tracking if individual is carrying stolen goods or weapons and describing how it outweighs privacy concerns).

[106] *See id.* (presenting law enforcement's response to fears surrounding RFID technologies in tracking individuals without their knowledge to weed out potential criminals).

GPS is another example of a cheap, wireless, machine-communication, which generates the location data of individuals.[107] Per *Jones*, law enforcement cannot simply engage in the warrantless monitoring of a suspected criminal's vehicle using GPS, but a GPS receiver remains "visible" and individuals can continue to be tracked indefinitely.[108] While commercially beneficial to the individual consumer and a helpful tool for law enforcement, GPS continues to pose a problem for those who wish to protect themselves from potentially unchecked monitoring, especially where the use of GPS spy-blocking jamming equipment is illegal.[109]

All of the above sensor technologies further the premise that in a world filled with these technologies, information can be captured in bulk and at random, to be reviewed and organized later.[110] People no longer collect information in real-time, and instead machines can simply collect data without any specific purpose or without the possibility to control private information when it manifests in the public sphere.[111] This lack of control of private information eliminates the possibility for the social concept of notice and consent to data collec-

---

[107] *See* Werbach, *supra* note 98, at 2333 (explaining GPS capabilities and benefits).
[108] *See Jones*, 132 S. Ct. at 949 (holding that warrantless monitoring by GPS is a "search" in violation of Fourth Amendment rights); *see also* Herbert, *supra* note 4, at 35 (explaining that four satellites continuously relay a person's location information by contacting a GPS receiver, and that receiver is always "visible").
[109] *See* Herbert, *supra* note 4, at 34 (showing the benefits of GPS technology); *see also* April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 666-67 (2005) (describing consumer benefits of GPS as well as detriments). *But see* Brief for the Respondent, *supra* note 103, at *6-7 (warning that individuals cannot protect their whereabouts from law enforcement when it comes to GPS without violating federal law).
[110] *See* Werbach, *supra* note 98, at 2347 (eliminating the idea of conscious surveillance and maintaining the challenge to address difficulties posed with sensor technologies in law).
[111] *See* Werbach, *supra* note 98, at 2347, 2353 (noting that "conscious actor[s]" are no longer necessary for surveillance where information is not gathered for a specific or conscious purpose, but collected in bulk, and data collectors do not control that information and are not responsible if it ends up in the public sphere); *see also* MICHAEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 200-01, (Alan Sheridan, trans., Vintage Books 2d ed. 1995) (1977) (laying out historical principles in Jeremy Bentham's Panopticon concept where surveillance should be "visible and unverifiable," elaborating that people are aware they are being watched but unaware of who is watching and when they are being watched).

tion.[112] These sensor technologies may ultimately "stretch the Katz framework," but this will be further explored in the next section of this Note.[113]

While proponents of smart dust focus solely on the benefits assured by the use of this technology, there are many possible detriments slowing the end-road toward development and actual integration into modern society.[114] The threat of privacy invasion is worsened by nanotechnologies like smart dust, and while Pister recognizes that there is a dark side to every technology, he simultaneously dismisses the threat as minor at best.[115] The military, environmental, and medical uses of smart dust all pose very real hazards that may potentially outweigh any benefits, and as mentioned, will be unwrapped in the next section of this Note.

IV. ANALYSIS

A. There *is* Privacy Available Within the Public Sphere

Individuals may be familiar with the concept that privacy is not absolute, but while it is a "slippery notion," seminal case law like *Griswold* and *Lawrence* solidify that individuals are in fact entitled to

---

[112] *See* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, N.Y.U., *archived at* http://perma.cc/RBH7-V96B (focusing specifically on notice and consent with online behavioral advertising but broadly addressing the inadequacies of notice and consent where tracking is inevitable and information can be obtained by third-parties).

[113] Werbach, *supra* note 98, at 2354 (explaining that outside of private spaces it is becoming more difficult to safeguard our public persona and the reasonable expectation of privacy test per *Katz* may be stretched and possibly reconsidered).

[114] *See* Nidhi Gupta et al., *Factors Influencing Societal Response of Nanotechnology: An Expert Stakeholder Analysis*, J. NANOPARTICLE RESEARCH (May 1, 2012), *archived at* http://perma.cc/V4GX-DBDM (performing expert analysis study of the possible benefits and detriments of nanotechnologies placing smart dust on lowest end of consensus spectrum for benefits in society, further discussing problem with introducing into society out of public fear); *see also* David Rejeski, *The Next Small Thing*, THE ENVIRONMENTAL FORUM, March/April 2004, at 42 (briefly stating possible problem of inhaling nanoscale particles into the lungs).

[115] *See* Pister, *supra* note 1 (stating "every technology has a dark side – deal with it" on smart dust webpage).

it.[116] The question remains: what privacy can be protected based on a person's or society's overall "reasonable expectations?"[117] While the argument is constantly made that there is simply no protection afforded to individuals within the public eye, privacy rights do not dissolve just because one walks down a street or goes out to dinner.[118] Yet smart dust, if released into the air, has the potential for constant surveillance and the monitoring of "everything," including last night's dinner selection.[119]

While a person may be well aware that any public action can be scrutinized, it is the extent to which they may be unknowingly watched which threatens their fundamental privacy rights.[120] Those unopposed to the prevalent use of surveillance technologies claim that in a society where sensors are largely used in the public eye, "no

[116] *See Lawrence*, 539 U.S. at 562 (ruling that "there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence"); *Griswold*, 381 U.S. at 485 (highlighting the undisputed right to privacy created by the Fourth Amendment); Koops & Leenes, *supra* note 5, at 123 (noting that privacy is a valued notion which predictably lacks clear boundaries).

[117] *See* Koops & Leenes, *supra* note 5, at 128 (addressing the concept of "reasonable expectation" of privacy); *see also Katz*, 389 U.S. at 359 (holding that an individual's right to privacy extends outside of his/her home, and that "he is entitled to know that he will remain free from unreasonable searches and seizures" by government wherever he may be).

[118] *See* Otterberg, *supra* note 109, at 664, 686-87 (arguing that while technology has broken down barriers between the public and private sphere, it is not impossible to maintain a semblance of privacy within public spaces); *see also Weaver*, 909 N.E.2d at 1200-01 (arguing that even a person riding as a passenger in a vehicle is entitled to privacy rights since it is a form of necessary travel).

[119] *See* Sutter, *supra* note 10 (describing smart dust as "electronic nerve endings for the planet" which can reflect constant real-time data about people); *see also* Kahn et al., *supra* note 77 (positing that smart dust prototypes may be small enough to be "buoyed by air currents" and remain suspended in the air, communicating for hours or days); Templeton, *supra* note 97 (posing the issue that smart dust could become airborne, given its small size).

[120] *See* Otterberg, *supra* note 109, at 686 (explaining that while a person may expect something revealed in the public to invite a bit of public scrutiny like glances from members of the public, they do not expect "highly individualized, targeted scrutiny…by law enforcement"). *But see* Koops & Leenes, *supra* note 5, at 132 (asserting that webcasting may establish a lower privacy standard, and thus poses the question of whether people may be "used" to being watched by web-radio).

private actor has the right to control what devices are used."[121] However, pervasive monitoring threatens the openness of society and smart dust is a contender for the further destruction of privacy rights where our moves are constantly recorded and revealed to law enforcement.[122] Regardless of the "careful placement" the creators intended for the technology, Pister and his team have said it themselves that smart dust may be so minute that it could be buoyed into the air – but it is where it lands that could present a problem.[123]

Justice Kennedy pronounced in *Lawrence* that "freedom extends beyond spatial bounds" resonating the idea that a person is free from government intrusion as they move about society.[124] Nanotechnologies like smart dust detract from our freedom to move about society without fear of detailed scrutiny into our private lives, interfering with our individuality, our autonomy, our dignity.[125] While the public may recognize that giving up some privacy contributes to important societal benefits, such as a reduced costs and increased security, technology like smart dust cannot be implemented without some risk of misuse and in this case, even physical harm.[126] As Justice Sotomayor noted in her concurrence in *Jones*, a relatively low-cost technology such as GPS allows for a low-cost monitoring of intimate information about a person, and can "alter the relationship between citizen and government in a way that is inimical to democratic society."[127]

---

[121] Werbach, *supra* note 98, at 2359 (claiming that companies seeking to prohibit private surveillance technology use on company grounds grant civilians little control over what technologies may be used within a public space).

[122] *See* Slobogin, *supra* note 6, at 408-09 (arguing that the openness of society may be threatened by pervasive monitoring).

[123] *See* Pister, *supra* note 76, at 4 (explaining that sensors do not have to be placed randomly into society or during military application); Kahn et al., *supra* note 77 (suggesting the possibility that smart dust can be suspended in the air by wind currents).

[124] *Lawrence*, 539 U.S. at 562 (expanding upon the concept of liberty as a fundamental right which extends beyond the home).

[125] *See* Koops & Leenes, *supra* note 5, at 135, 140 (addressing core values protected by privacy rights and identifying smart dust as covert, perfect tracking technology threatening the same).

[126] *See* Koops & Leenes, *supra* note 5, at 136 (relaying that giving up a part of one's private sphere contributes to other important societal values).

[127] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (2011) (Flaum, J., concurring)).

B. Smart Dust Threatens Fundamental Privacy Rights and Public Health, Expanding Upon Known Threats by Other Sensor Technologies

As Justice Brandeis remarked in his *Olmstead* dissent, "clauses guaranteeing the individual protection against specific abuses of power, must… [adapt] to a changing world."[128] While multiple sensor technologies offer a variety of commercial and government benefits, the smaller they become and the more sophisticated they become warrants greater protection and further diminishes privacy rights.[129] Mirroring the constant surveillance capabilities of GPS, the low-cost and miniature size of RFID, and the imaging and sound capabilities of camera surveillance, smart dust is a pervasive threat combining all of the benefits and detriments of these technologies into one super-technology.

Smart dust is a driving force in what commentators are deeming the "new industrial revolution."[130] This revolution of information and biometric technology wrapped up into a nanotechnology device may very well explode into major scientific developments, but the unknown impact could render adverse consequences.[131]

While smart dust presents multiple advantages in the field of environmental law, such as measuring atmospheric weather conditions and studying the ecosystem to detect environmental toxins, its small size poses some very real hazards.[132] Nanoscale particles can lead to disastrous consequences if they are inhaled deeply into the

---

[128] *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting).

[129] *See* Werbach, *supra* note 98, at 2329, 2335, 2340 (addressing the tiny sensor devices prevalent in RFID and GPS technologies as well as both benefits and detriments, and explaining that privacy law becomes undermined with these technologies).

[130] *See* Rejeski, *supra* note 114, at 42 (claiming nanotechnology is paving the way for such a revolution); *see also* GRAD, *supra* note 11 (describing nanotechnology as a "trailblazing notion" that has attracted significant scientific attention and is part of a new era).

[131] GRAD, *supra* note 11 (summarizing Rejeski's explanation of the "new industrial revolution" but cautioning that this new area yields questions and policies for study and debate).

[132] *See* GRAD, *supra* note 11 (outlining the benefits of the use of smart dust in the environment but warning that the risks are yet to be identified).

lungs or cross over into the blood-brain barrier.[133] Though one benefit of smart dust is proposed as more efficient brain studies, inserting a drug-carrying nanoparticle can cause brain damage or affect the absorption of brain nutrients if executed unsuccessfully.[134] Further, particles released into the air and accidentally inhaled can inflict lung injuries and damage other bodily organs and functions.[135]

Since smart dust is only in the beginning proposal stages, the apparent privacy threats and economic threats should be judged from the concerns posed by other sensor technologies. Just as smart dust is marketed as a relatively inexpensive and miniature technology, so small that it cannot be seen, RFID chips are also cheap, attractive technologies that have prompted public concern.[136] While smart dust and RFID chips serve different purposes where RFID tags items to monitor criminal activity and ensure citizens are law-abiding, and smart dust acts as stationary, versatile computer systems that thrive in detection and monitoring, both are aimed toward beneficial societal contribution.[137] Both technologies are wireless communications devices that communicate with machines to monitor and detect information and relay the same to government or law enforcement.[138] Yet, just as RFID positively serves society, the 'two sides to every coin' argument is not unmerited where searches may be performed on people without their knowledge, echoing "unconscious surveillance."[139]

---

[133] *See* Rejeski, *supra* note 114, at 42 (presenting hazards of smart dust due to its small size); *see also* GRAD, *supra* note 11 (describing the same risks).
[134] *See* GRAD, *supra* note 11 (discussing findings of brain studies and the risks associated with the use of smart dust).
[135] *See* GRAD, *supra* note 11 (identifying adverse effects of inhaling nanoparticles).
[136] *See* Werbach, *supra* note 98, at 2331 (describing privacy concerns provoked by RFID, but also emphasizing its benefits).
[137] *See* Christiana et al, *supra* note 105 (identifying the potential RFID technology carries in aiding law enforcement to prevent against stolen property); Templeton, *supra* note 97 (proposing possible uses for smart dust and its capabilities including becoming airborne and detecting information from afar).
[138] *See* Christiana et al, *supra* note 105 (noting that RFID serves an important function of tracking in order to aid law enforcement); Templeton, *supra* note 97 (affirming that the possible applications of smart dust likely hinge on detection and monitoring and describing smart dust as a wireless communication); Werbach, *supra* note 98, at 2330 (pointing out that RFID is a wireless sensor).
[139] Werbach, *supra* note 98, at 2355, 2357 (emphasizing "unconscious surveillance" involving satellite or aerial photography occurring throughout society); *see*

Though law enforcement officials believe that surveillance technologies like RFID pose no threat when used carefully and legally operated, they still worry about the ability of criminals to essentially pick-pocket information from individuals that is stored on RFID devices.[140] While the Fourth Amendment "search" is only considered a violation if there is government fault, and while usually there is no legal "search" if information is extracted in the public sphere, certain law enforcement officials have concurred that RFID scanning adequately fits the category of "search" and contend that restrictions on its use are necessary.[141] While RFID is a poster-technology for monitoring commercial inventory and promoting safety and security, the constant tracking of personal information qualifies as a potentially invasive use, contributing to the declining fundamental privacy rights of the public-at-large.[142] Likewise, smart dust, an up-and-coming, omnipresent technology with proposals to scatter it throughout society, in addition to its use in science labs or by government agencies, presents a serious threat for government or individual manipulation or misuse.[143] This scenario mirrors Roger Clarke's theory of dataveillance, a world without anonymity or privacy.[144]

---

also FOUCAULT, *supra* note 111, at 201 (arguing that surveillance should be "visible and unverifiable," introducing the theory of unconscious surveillance which seems ahead of Foucault's time); Christiana et al, *supra* note 105 (addressing privacy concerns among the public).

[140] *See* Christiana et al., *supra* note 105 (responding to questions regarding criminal uses of RFID).

[141] *See* Sommer, *supra* note 104, at 65 (summarizing the history of the Fourth Amendment and how it is inapplicable within public spaces and when a "search" is performed by a private entity and not government). *But see* Christiana et al., *supra* note 105 (asserting that while RFID is mostly non-intrusive, RFID scanning by government would still be a "search" in violation of the Fourth Amendment and must be monitored carefully).

[142] *See* Sommer, *supra* note 104, at 52 (presenting information that as developers refine the RFID technology, it is becoming more pervasive and invasive within society).

[143] *See* Froomkin, *supra* note 6, at 1470-71 (introducing the idea of dataveillance and explaining that easy government access to all facets of an individual's personal information serves as a criminal deterrent, but also results in misuse where people will be under constant scrutiny before crimes even occur); *see also supra* Part IV.B. (outlining proposals for smart dust's use which are ultimately detrimental to society).

[144] *See* Froomkin, *supra* note 6, at 1470-72 (defining dataveillance and potential dangers). Dataveillance is the collection of large amounts of personal data that

While GPS is also a commercially-driven device designed for both consumer use and criminal deterrence, opponents are concerned with its capabilities to totally substitute the senses of law enforcement officers.[145] While this technology offers many benefits, like quick detection of consumer locations in emergency situations and provides navigational assistance as well as employee monitoring, GPS eliminates even the little bit of anonymity a person has left within the public sphere, providing an "all-seeing eye" for individual actions.[146] The indefinite monitoring periods prevalent by the use of GPS echo the proposed indefinite periods of monitoring made capable by smart dust.[147] With the concept of dust motes floating in the air without a fixed location, the engineering researchers behind smart dust are trying to create constant communication between the sensors and base-station transceivers without interrupted lines-of-sight.[148] Just as GPS

threatens individual autonomy and harms society, where the law will be applied inadequately and may even result in witch-hunts for those who fit a certain data profile. *See* Froomkin, *supra* note 6, at 1466, 1471-1472 (explaining the impact of dataveillance on an individual and societal level). Dataveillance ultimately makes privacy impossible and is one of the reasons that staying hidden even while home surfing the Internet allows for no anonymity. *See* Froomkin, *supra* note 6, at 1472, 1482 (discussing the possibility of total lack of privacy due to rising surveillance technologies and data collection).

[145] *See* Brief for the Respondent, *supra* note 103, at *29, *32 (cautioning that GPS is distinctive from visual surveillance and a gross privacy violation). This Brief arising from the *Jones* matter argues that like the thermal imaging presented in *Weaver*, GPS goes beyond the "natural sensory capacities of law enforcement" and "facilitates a new technological perception of the world" where anyone can be followed indefinitely. *See* Brief for the Respondent, *supra* note 103, at *29 (quoting *Weaver*, 909 N.E.2d at 1199).

[146] *See* Otterberg, *supra* note 109, at 666-67 (offering examples of many benefits of GPS). *But see* Brief for the Respondent, *supra* note 103, at *30 (recognizing that one can still maintain anonymity in the public sphere, for example, averting eyes from passersby on the sidewalk, but GPS is analogous to an unblinking eye constantly scrutinizing individuals).

[147] *See* Otterberg, *supra* note 109, at 667-68 (explaining that certain batteries used in GPS can allow for monitoring either weeks at a time or visual "round-the-clock surveillance"); Whitwam, *supra* note 11 (proposing that the use of intelligent dust for brain studies has the potential to "act like an MRI running in your brain all the time").

[148] *See* Kahn et al., *supra* note 77 (relaying the science behind non-latent dust motes and how to get information without signals being interrupted). The researchers describe using a "multihop routing" method through the use of multiple tiny sensors which relay information from one sensor to the other when a line-of-sight is

is a technological weapon in the field of law enforcement where it generates exact locations and accurate records of individual movement, smart dust could be manipulated by law enforcement to perform "covert surveillance…on unsuspecting citizens."[149]

Smart dust, designed with versatile applications in mind so that it can be strategically placed on an object, within an area, or attached to a vehicle in which the government wishes to monitor, and designed with the intent that it can be suspended into the air, is similar to aerial surveillance.[150] While the uses of smart dust vary, its creators have confirmed that it has environmental and biological uses, among others.[151] However, while one smart dust application may be air dispersion, the duration of its surveillance and capability for "blanket" surveillance over society, echoes similar concerns spurred by prolonged aerial surveillance.[152]

While aerial surveillance over the public would not generally be considered a Fourth Amendment "search," the Supreme Court has voiced its concern that aerial surveillance has the ability to become a "search" if conducted in a hazardous way, or in ways which interfere with the privacy of the home.[153] Depending on a particular vantage point of a surveillance device, it could have the potential to intrude upon a private space, and this concern is relevant to the unknown

blocked, providing continuous monitoring. *Id.* (explaining "multihop routing" to decrease sensor latency overall).

[149] *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring); *see also* Brief for the Respondent, *supra* note 103, at *12 (arguing smart dust technologies have the capability to assist in surveillance operations on average individuals without their consent).

[150] *See* Kahn et al., *supra* note 77 (describing ways in which smart dust technology could be utilized).

[151] *See* Kahn et al., *supra* note 77 (listing multiple proposed uses for smart dust technology including but not limited to recording data for geological or physiological purposes, and military perimeter surveillance for chemical detection).

[152] Brief for the Respondent, *supra* note 103, at *12 (maintaining stance that smart dust could be used for covert surveillance of individuals); *see also* Slobogin, *supra* note 6, at 389-92 (relaying concerns by courts that aerial surveillance has the potential to be invasive and unconstitutional if prolonged);

[153] *See* Slobogin, *supra* note 6, at 397-98 (citing Florida v. Riley, 488 U.S. 445, 446 (1989)) (finding no "search" where there was no reasonable expectation of privacy or home interference when helicopter surveillance revealed marijuana growing in greenhouse).

placement of smart dust technology.[154] Smart dust's extremely small size is also a worrisome, hazardous characteristic since small particles in the air can be deeply inhaled in the lungs and carried to the home of the person which inhaled them.[155]

As the presence of surveillance and sensor technologies rapidly increases in society, they are becoming a norm in police investigations within our "ambient information environment" and are contributing to the dissolution of fundamental privacy expectations.[156] The more the public is aware that the government collects people's personal information through the use of these surveillance technologies, the less the public may expect immunity from privacy right violations and may even accept such violations as warranted.[157] It is becoming rarer for individuals to not be tracked by government or law enforcement, given ubiquitous surveillance technologies.[158] However, when it comes to "unconscious surveillance" scholars have noted that controversies are sure to emerge, suggesting that individuals may have cause to worry.[159]

---

[154] *See* Slobogin, *supra* note 6, at 399 (arguing that lawful or unlawful vantage points of surveillance technologies can make all the difference when determining Fourth Amendment violations).

[155] *See* GRAD, *supra* note 11 (noting that the small size of smart dust poses potentially harmful problems).

[156] Werbach, *supra* note 98, at 2354-55 (explaining that surveillance and sensor technologies like camera-phones and RFID are so commonplace that Fourth Amendment arguments and the reasonable expectation of privacy ideals are broken down); *see also* Part IV.B. (describing detriments and reduced privacy expectations due to the emergence of sensor technologies).

[157] *See* Werbach, *supra* note 98, at 2355 (expanding upon the public's lessened expectations of privacy given that society has become an "ambient information environment"); *see also* RULE, *supra* note 9, at 182 (recognizing that citizens have grown accustomed to widespread surveillance and to "'choosing' discrete losses of control over [their] data in exchange for the trappings of normal life in an information-hungry world").

[158] *See* Werbach, *supra* note 98, at 2354 (cautioning that surveillance technologies are constantly recording and tracking people's actions outside of private spaces).

[159] Werbach, *supra* note 98, at 2355, 2357 (offering examples of unconscious surveillance with the rapid production of technologies like RFID and asserting that controversies are a likely result); *see also* RULE, *supra* note 9, at 182 (explaining that when individuals succumb to the widespread collection of their personal data and acknowledge it as an everyday occurrence, people "incrementally nudge that world toward total surveillance").

A prevalent concern with surveillance technologies is that social norms must adapt to the presence of these technologies within society.[160] In this free-information age, while state and federal government cope with how to best use cutting-edge technologies like smart dust and attempt to create suitable law, it is the individuals within each community that must wrestle with accepting the loss of privacy or protecting their fundamental rights, albeit with difficulty.[161] "We are…in a transitional period" where the prevalence of networks of tiny sensors is becoming strenuous to regulate.[162] The near-invisible characteristic of smart dust mirrors a concept known as the Polyopticon, "a world in which everyone can watch."[163] Data collection fosters data sharing – the continuous collection of information described by Pister and his colleagues, without explanation on smart dust's limitations or proposed regulations, conjures up the need for adequate restrictions as this technology fully integrates into society.[164]

---

[160] *See* Werbach, *supra* note 98, at 2367 (asserting that the most significant responses from surveillance technologies appear in the form of changing social expectations and etiquette).

[161] *See* Werbach, *supra* note 98, at 2370 (explaining that conscious efforts to limit the spread of information and prevent privacy intrusions will be difficult).

[162] Werbach, *supra* note 98, at 2361, 2365 (introducing the topic of legal regulations and difficulties posed).

[163] *See* Werbach, *supra* note 98, at 2362-63 (developing ideas of a "transparent society" where pervasive, countless sensor technologies intrude upon basic privacy expectations). The "transparent society" is reflected in early concepts coined by English philosopher Jeremy Bentham and his Panopticon theory. Bentham describes the ancient emergence of surveillance society as embedded within old prison systems where one person in a guard-tower watches everyone around him who are the prisoners, and they are barely exposed to light, hidden to the fact that their every move can be seen. *Id.* (describing the history of philosophical interpretations of surveillance societies); FOUCAULT, *supra* note 111, at 200-01 (explaining the layout of Bentham's Panopticon and its overall purpose to employ "conscious and permanent visibility"). The Polyopticon expands upon this concept as applied in the modern world, where there is not one figure in a watchtower but numerous surveillance entities, via online platforms or advanced technology, which constantly collect information away from public view. *See* Werbach, *supra* note 98, at 2363 (defining the Polyopticon and its dangers).

[164] *See* Werbach, *supra* note 98, at 2363 (shedding light on traditional concepts of surveillance technology and the current state of society where information is shared easily among people).

C. A Need for Government Regulation and Suggested Proposals

With smart dust only in the very early stages of its production, it is tough to determine both the overall public and government reaction to its assimilation into society. In her *Jones* concurrence, Justice Sotomayor further expanded upon the misuse of surveillance technologies, claiming that regardless of the lawfulness of the government in obtaining an individual's personal information, people should not reasonably expect their movements to be recorded "in a manner that enables the Government to ascertain . . . their political and religious beliefs, sexual habits, and so on."[165] The discreet presence of smart dust and other surveillance technologies allows for arbitrary intelligence collection "cloaked in the greatest secrecy."[166] While the government has succeeded in ample regulation for wiretapping, nanotechnologies, at the forefront of their introduction into American society, warrant greater privacy protections to avoid the erosion of privacy rights altogether.[167]

An important issue with the rampant presence of surveillance technologies is disclosure of their use to the public.[168] The American Bar Association ("ABA") Task Force, in finalizing its Standards Concerning Technologically-Assisted Physical Surveillance, determined that the public is entitled to at least "reasonable notice" of covert surveillance by law enforcement, which could ease the presence of smart dust in society.[169] While many opponents argue for the ban of nanotechnologies like smart dust altogether, such a harsh legal restriction can be mitigated by adequate public disclosure.[170] Specif-

---

[165] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).
[166] Young, *supra* note 6, at 1044-46 (urging for judicial regulations where surveillance technologies allow for great misuse by law enforcement).
[167] *See* Young, *supra* note 6, at 1057-58, 1062 (reporting an overall trend in legislative erosion of privacy interests).
[168] *See* Slobogin, *supra* note 6, at 410-11 (outlining ABA attempts with other surveillance technologies to prevent unlawful use through disclosure).
[169] *See* Slobogin, *supra* note 6, at 434 (describing resolutions by the ABA Task Force); Sommer, *supra* note 104, at 58 (arguing specifically in the case of RFID that an outright ban is unnecessary when there are effective ways to mitigate any negative effects it may carry).
[170] *See* Werbach, *supra* note 98, at 2358 (asserting that the first response to any unwanted sensors is a proposal or attempt to ban them).

ic concerns addressing RFID technology have led proponents to argue for regulations such as notice and consent, where consumers are given notice of the existence of RFID tags on items, and subsequent consent by making a purchase.[171] While smart dust has not been proposed as an entirely commercial technology, researchers do anticipate it as a civilian tool, and notice and consent may be a relevant restriction to apply where people can consent to smart dust's existence by merely walking in a public space that warns of the presence of miniature sensors, through signage or other mediums.[172]
Where nanotechnology presents some harmful risks, specifically in environmental and scientific applications, testing its safety is a crucial regulation.[173] As noted by Kevin Ausman, the executive director of the Rice University Center for Biological and Environmental Nanotechnology, "the traditional approach of new technologies to environmental concerns is to wait until there is a problem."[174] As the hype surrounding smart dust and any subsequent concerns may be premature, one sure way to quell negative environmental impacts is proactive testing and simultaneous public disclosure.[175]

Finally, while multiple applications for smart dust are proposed, the ultimate aim to achieve total transparency increases the risk of misuse, and the ABA has warned that particularly invasive technologies must have a very limited use.[176] Allowing potential surveillance to occur at a great distance from or shielded from the public, combined with the use of a technology that is not widely

---

[171] *See* Sommer, *supra* note 104, at 58 (explaining mitigation of concerns through notice and consent regulations).
[172] *See* Kahn et al., *supra* note 77 (mentioning specific applications for smart dust as both civilian and military use); *see also* Sommer, *supra* note 104, at 58 (ensuring consumers receive proper notice and issue consent through the specific purchase of a product with an RFID tag made known to them).
[173] *See* GRAD, *supra* note 11 (stating that proponents of the development of nanotechnology should encourage safety testing efforts).
[174] GRAD, *supra* note 11.
[175] *See* GRAD, *supra* note 11 (explaining that the new technologies are successful based on early decisions and development, and any hazards or potential dangers should be voiced to the public).
[176] *See* Young, *supra* note 6, at 1044-45 (urging that discreet surveillance technologies should only be used in limited circumstances, if at all); *see also* Chebaclo, *supra* note 7, at 146 (presenting ideas of public paranoia as sufficient deterrent factor for preventing misuse accompanying unknown surveillance technologies and perhaps fostering regulations).

known, poses constitutional threats where there could be misuse and largely decreased government accountability.[177] Limiting smart dust's use in society, versus its rather versatile proposed applications, may be an effective restriction in preventing privacy invasions.

V. CONCLUSION

Even as we move about in public we expose a hint of our private selves. Smart dust ensures that the government has an all-seeing, infinite eye. Though smart dust carries many benefits for the greater good of society, it may be implemented at the risk of exposing innocent information people just do not want revealed, and it could also cause bodily harm. Given the controversies surrounding other technologies such as thermal imaging, wiretapping, camera surveillance, RFID, and GPS, smart dust may be the newest technology to come knocking on the chambers of the Supreme Court justices. A person's reasonable expectation of privacy does not equate to constant, infinite surveillance by government and Fourth Amendment privacy protections are threatened where this surveillance remains unchecked.

Privacy is a fluid, "changing thing"[178] and it must be re-addressed whenever a technology of this modern scale enters into society. While researchers and government could dream up a slew of possible regulations and restrictions such as weather studies in enclosed areas, creating time-limited sensors or possibly even biodegradable sensors so privacy is only minimally infringed upon, the best methods will only be revealed as the production of smart dust becomes a mainstream reality. The government should not have to eliminate smart dust, but regulations should be on the top of its list to overcome any potential Fourth Amendment privacy violations. Where something so small could end up in the wrong hands, and where it will be difficult for the public to adapt to an unseen and unknown sensor floating throughout society, limitations on the use of smart dust are crucial to calm arguments by conspiracists, scholars,

---

[177] *See* Young, *supra* note 6, 1069-70 n.305 (asserting that new science technologies that are largely unknown may pose constitutional threats).

[178] Koops & Leenes, *supra* note 5, at 132 (explaining that privacy is dependent on socio-cultural factors and is a fluid concept).

and average citizens, and to prevent possible future litigation. As society improves and adapts, so must its applicable laws.