12-1-2000

Chipping Away at the Boundaries of Privacy: Intel's Pentium III Processor Serial Number and the Erosion of Fourth Amendment Privacy Expectations

George M. Dery III

James R. Fox

Follow this and additional works at: http://readingroom.law.gsu.edu/gsulr

Part of the Law Commons

Recommended Citation

This Article is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact jgermann@gsu.edu.
GEORGIA STATE UNIVERSITY
LAW REVIEW

VOLUME 17    NUMBER 2    WINTER 2000

CHIPPING AWAY AT THE BOUNDARIES OF PRIVACY: INTEL’S PENTIUM III PROCESSOR SERIAL NUMBER AND THE EROSION OF FOURTH AMENDMENT PRIVACY EXPECTATIONS

George M. Dery III†

James R. Fox††

INTRODUCTION

Imagine a world in which the government had the potential power to observe and record your every public act. What if law enforcement, whether the local police or a federal agency, could keep tabs on every store you visited in the mall, each book you glanced through at the bookstore, and all the outfits you tried on for size? The government would have a permanent record of the dates and places of the businesses you patronize, the items you peruse, and therefore, albeit indirectly, the thoughts you ponder. If police followed you to each store, restaurant, gym, and bar, and then videotaped you as you shopped, ate, worked

† Associate Professor, California State University Fullerton, Department of Political Science/Criminal Justice. Former Deputy District Attorney, Los Angeles, California. B.A., 1983, University of California Los Angeles; J.D., 1987, Loyola Law School, Los Angeles.

†† Systems Analyst, Structural Bioinformatics, Inc. B.A., Criminal Justice, summa cum laude, California State University Fullerton. J.D. candidate, 2005, University of San Diego.

331
out, and met with friends, such constant surveillance would be considered by many to be police harassment.

Yet, such intrusive monitoring and recording of every individual’s activity is achievable, and in a sense, likely. The surveillance also will come cheaply; no army of field agents or continuously running cameras are required. Instead, the government can simply sit passively and wait for most of us to buy the newest personal computers on the market, equipped with the Pentium III chip, and use them to become increasingly reliant on Internet commerce.

Each Pentium III microprocessor chip is serialized with a unique 96-bit number. This number enables Internet businesses to go beyond the kind of information they have collected in the past (namely, kind of computer, amount of memory, and modem speed) and instead pinpoint an actual computer on a desk. An analogy may be made to cars. Now, a fast food employee may know he is preparing a meal for a person in a 1999 Ford Mustang. However, if the employee came out to the drive through and wrote down the car’s Vehicle Identification Number (VIN), the employee could pinpoint the actual car the customer was driving. Likewise, a company on the Internet will know the precise computer with which it is dealing. Such precise identification may not seem significant if, as with cars, all computers did was transport us to various destinations. But computers, of course, do much more. In this information age, computers connected to the Internet allow users access to online shopping, browsing, banking, and chatting.

Intel had the best of motives in creating such a chip; the number provides corporate information technology departments with a tool to "track assets and manage systems in a more efficient manner to help reduce total cost ownership." Consumers also benefit: "For consumers, the potential of the Internet promises new ways to shop online, manage their lives, and access and share information." Yet the very number used to promote e-commerce may in turn create the possibility of severe government intrusion on privacy. A number that helps a supplier anticipate an individual consumer's needs may also enable the government to apprise itself of a citizen's whereabouts and activities on the Internet, regardless of the intimate nature of the transaction.

Intel has been sensitive to consumers' concerns and has aimed to address them. The chipmaker has built the Pentium III so that its serial number can be switched off. Furthermore, Intel has encouraged computer manufacturers to ship the chip in the "off" position. Moreover, Intel advises that the "off" switch operates at the Basic In Out System (BIOS), the most fundamental level of a computer's operation, so that outsiders cannot turn the chip back on. Yet, as will be discussed below,

---

5. Id.
6. Intel has informed its consumers:
With the introduction of the Pentium III processor, Intel has also introduced a utility that allows users to control their processor serial number . . . . The Intel processor serial number control utility is a Windows program that enables or disables the reading of the Pentium III processor serial number by software. This allows users to control which software programs or Web sites have permission to read the processor's serial number and ensures that their preference for the processor serial number setting is enforced. The default setting of the utility is to disable the reading of the processor serial number.

Intel's cautious measures, however elaborate and well-meaning, appear to be vulnerable to circumvention.\(^9\)

If Intel's security measures can be defeated, Intel's Pentium III chip continues to be the nation's most popular chip,\(^10\) and Internet commerce continues to grow, then a computer's individual serial number may become an easily accessible bit of information in an increasingly growing part of the world's economy. This may reduce the reasonableness of a privacy expectation in the serial number of the computers most people use in conducting their business and lives on the Internet, and this reduced expectation may in turn alter the scope of privacy covered by the Fourth Amendment.

This Article begins by exploring the serialization of the Pentium III chip. Part II presents an overview of the scope of Fourth Amendment application. This discussion includes a review of the Supreme Court's "reasonable expectation of privacy" definition for Fourth Amendment searches, an examination of the impact private conduct has on the scope of the Fourth Amendment protection, and the Court's tendency to equate the potential of a privacy breach with a reduction in reasonable expectations. Finally, Part III critically assesses the probable effect that Intel's chip will have on privacy rights.

I. INTEL'S PENTIUM III SERIALIZATION

Intel's Pentium III processor serial number (PSN) was originally created to solve existing problems. Cyberspace is not immune from the woes facing the tangible world. On the Internet, an individual's or a company's security may be compromised, digital content may be pirated, and chips may be stolen or counterfeited.\(^11\) In response, Intel embedded the PSN into its

9. Zero Knowledge Systems has designed a "Trojan horse" which makes the serial number available even when initially turned off. See Adam Creed, Software Bypasses "Switched Off" Pentium Chip IDs, Newsbytes News Network, at http://www.elibrary.com (Mar. 11, 1999); Craig Menefee, Symantec Blocks Zero Knowledge P-III Crack, Newsbytes News Network, at http://www.elibrary.com (Mar. 19, 1999); see also infra notes 27-30 and accompanying text.

10. Intel is the world's largest chipmaker. See Kornblum, supra note 3.

Pentium III chip "during the manufacturing process." Intel "claims that the serial number will facilitate e-commerce, promote 'digital content protection,' prevent counterfeiting of Intel processors, and help to track stolen ones." Hard-wired into each Pentium III chip, the PSN is a "persistent, non-modifiable identifier, which applications can use to provide stronger identification of the processor and, with similar identification factors such as username and password, the system and user." Within months of Intel's creation of its new chip, twenty-five companies created "applications optimized for the processor serial number."

Efficiency in identification came at a price. To many observers, the result of Intel's innovation was a situation in which a person's CPU (central processing unit, or chip) electronic serial number can now be used in ways that are hostile to the user's best interests. Specifically, privacy advocates see a dark future in which "e-commerce sites—and anyone else who may be interested—[will] track users as they make their way around the World Wide Web. They warn that companies who collect such information could merge their files to create detailed personal records of computer users." Jason Catlet, president of Junkbusters, a technology lobbying group, has sounded a particularly ominous note, declaring: "The PSN is the greatest threat to the privacy of the American consumer since the Social Security number."

---

1999, at 5, available at http://www.elibrary.com. Some of the impetus behind serialization has come from groups pressuring Intel to address security concerns:

A variety of interests have been pestering Intel for some time to provide each computer with a unique identifier. Although the current debate most often names purveyors of electronic commerce as the main source of pressure (site operators want to add a level of security to transactions), corporate information technology managers and software developers have also been knocking on Intel's door.


14. See Martinez, supra note 2.
15. PSN Technical Notes, supra note 2.
16. Savage & Tiazkun, supra note 11.
17. See Glass, supra note 11.
18. Martinez, supra note 2.
Intel has not ignored these privacy concerns. In fact, the chipmaker has responded by introducing a software utility that gives users control over their processor serial number.\textsuperscript{20} Further, the computer user is continually aware of the PSN's "on/off" status, because "[t]his utility places an icon in the Windows system tray to provide the user with a visual indication of the state of the processor serial number feature."\textsuperscript{21} Also, it is difficult to mistakenly activate the PSN while using the computer because "enabling the serial number requires the system to be restarted."\textsuperscript{22} Thus, Intel designed its utility to allow any user the ability to: (1) determine whether the processor serial number is enabled or disabled; (2) enable or disable processor serial number; and (3) read the value of the processor serial number.\textsuperscript{23}

To ensure wide availability, Intel provides the corrective software utility in a variety of forms. Users can download the utility from the Intel Web site and manufacturers' Web sites. Intel also offers a CD-ROM.\textsuperscript{24} Intel has been so conscientious that, although the utility was originally offered as a Windows program, Intel vowed to work with the makers of other operating systems, such as Linux, to develop capabilities for the processor serial number.\textsuperscript{25} Moreover, the chipmaker is currently offering its privacy patch in a variety of languages, including English, German, Japanese, Portuguese, Korean, and two versions of Chinese.\textsuperscript{26}

However, Intel's efforts, while laudable, failed to solve the core problem: privacy. In March 1999, software developer Zero-Knowledge Systems announced that it had "designed a program that can easily bypass Intel Corp.'s Pentium III serial number control utility and access the computer user's serial number."\textsuperscript{27}

\begin{itemize}
  \item[20.] See supra notes 6-8 and accompanying text.
  \item[21.] PSN Overview, supra note 6.
  \item[22.] Id.
  \item[23.] See PSN Technical Notes, supra note 2.
  \item[24.] See PSN Overview, supra note 6.
  \item[25.] See id.
  \item[27.] Creed, supra note 9.
\end{itemize}
Zero-Knowledge Systems' president, Austin Hill, stated:

Intel claims its utility will turn off the serial number and alert you when it has been turned back on.... Our research shows that Intel’s patch can actually leak out your serial number even when it tells you that you’re safe. We are very concerned about the public's ability to protect their privacy while using a Pentium III.\textsuperscript{23}

So concerned, apparently, that Zero-Knowledge Systems has set up a Web site “where Pentium III users can test the exploit themselves.”\textsuperscript{29}

Next in the see-saw battle, Symantec announced it had blocked a Zero-Knowledge Systems' crack of Intel's Pentium III serial number blocking utility.\textsuperscript{30} Thus, the battle over the privacy concerns has simply moved to a new level.

Intel executives might rightfully wonder if any good deed goes unpunished. David Banisar, policy director at the Electronic Privacy Information Center, called for a recall of Pentium III chips, stating that Intel’s Pentium III chips “function better protecting Intel’s public image than consumer’s privacy.”\textsuperscript{31} Junkbusters’ president, Jason Catlett, was even less forgiving, calling Intel’s actions “sleight of hand.”\textsuperscript{32}

However harsh, the criticism of Intel may illuminate one nagging truth: A privacy flaw in hardware cannot be remedied completely by a software fix. As previously noted, Intel’s 96-bit processor serial number is immutable—it is burned into the chip.\textsuperscript{33} In contrast, Intel’s privacy patch is software-based, and as Intel itself has conceded, “[a]ll software can be attacked and compromised with enough time and effort.”\textsuperscript{34} Thus, the potential for privacy invasion via Intel’s PSN is ever present.

\textsuperscript{28.} Id.
\textsuperscript{29.} Id.
\textsuperscript{30.} See Menefee, supra note 9.
\textsuperscript{31.} Creed, supra note 9.
\textsuperscript{32.} See Moore, supra note 7.
\textsuperscript{33.} See supra note 2 and accompanying text.
\textsuperscript{34.} PSN Q & A, supra note 4.
II. THE DEFINITION OF A FOURTH AMENDMENT SEARCH

When the Framers of the United States Constitution crafted the Fourth Amendment, they limited its reach. By its terms, the amendment applies only to "searches and seizures." Therefore, to be heard on a Fourth Amendment claim, a litigant must first establish that the intrusion he or she suffered was a "search" or a "seizure" within the meaning of the Constitution. The Supreme Court deemed this threshold issue so significant that failure to meet it has often been dispositive of the outcome. Further, our nation has witnessed the Court embark on a curious odyssey in its quest to determine what a Fourth Amendment search actually is.

A. The "Reasonable Expectation of Privacy" Rule

The notion that a computer chip can alter the boundaries of constitutional privacy is fitting, since much of the Court's precedent defining a Fourth Amendment search has involved responses to advances in technology. The Court itself has reviewed the technological evolution of surveillance and the law's reaction to the resulting threats to privacy. In Berger v. New York, Justice Clark led the Court's search discussion back to the common law nuisance of eavesdropping, where the intruder listened "by naked ear under the eaves of houses or their windows, or beyond their walls seeking out private discourse." Such an "undignified" method could not avoid a

35. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

36. See California v. Greenwood, 488 U.S. 35 (1988) (holding that the nonexistence of a Fourth Amendment search was dispositive); see also Soldal v. Cook County, Ill., 508 U.S. 56 (1992) (reversing the Court of Appeals for its failure to recognize a seizure of an item); California v. Hodari D., 499 U.S. 621 (1991) (finding it dispositive that the officer had not seized the defendant's person).


39. Id. at 44-45.
certain "awkwardness," perhaps being caught outside another's window.\textsuperscript{40} However, technology addressed such inefficiency. Electricity's technological advances, particularly the telegraph, enabled "surreptitious interception of messages" by everyone from Civil War spies to newspaper competitors to racetrack bettors.\textsuperscript{41} The next technological advance brought with it further intrusions on privacy. "[T]he telephone brought on a new and more modern eavesdropper known as the 'wiretapper.'"\textsuperscript{42} The Court first confronted wiretapping in\textit{ Olmstead v. United States}.\textsuperscript{43} In\textit{ Olmstead}, prohibition agents tapped several phone lines, including Roy Olmstead's, to collect evidence of bootlegging.\textsuperscript{44} Since the federal government made its taps "in the streets near the houses" rather than inside subjects' homes, the Court characterized the intrusions as "made without trespass upon any property of the defendants."\textsuperscript{45} The\textit{ Olmstead} Court then made the simplistic equation that no physical trespass meant no search within the meaning of the Fourth Amendment.\textsuperscript{46} The next technological step in surveillance was the miniature microphone, or "bug."\textsuperscript{47} When confronted with this technology, the Court seemed truly awed by its power. In\textit{ Berger}, Justice Clark described bugs as "[n]o larger than a postage stamp—these gadgets pick up whispers within a room and broadcast them half a block away to a receiver."\textsuperscript{48} Despite its recognition of a bug's intrusive abilities, the Court initially failed to adequately assess the implications of the new technology. In\textit{ Goldman v. United States},\textsuperscript{49} a case involving possible violation of bankruptcy laws, federal agents placed a "detectaphone" against a wall to hear the defendant make incriminating statements in the next office.\textsuperscript{50} The Court, again

\begin{itemize}
\item\textsuperscript{40} See id.
\item\textsuperscript{41} See id. at 44-47.
\item\textsuperscript{42} Id. at 46-47.
\item\textsuperscript{43} 277 U.S. 438 (1928).
\item\textsuperscript{44} See id. at 456-57.
\item\textsuperscript{45} Id. at 457.
\item\textsuperscript{46} See id. at 486.
\item\textsuperscript{47} See Berger, 388 U.S. at 46-47.
\item\textsuperscript{48} Id.
\item\textsuperscript{49} 316 U.S. 129 (1942).
\item\textsuperscript{50} See id. at 131-32.
\end{itemize}
tying its Fourth Amendment search definition to physical entry upon a constitutionally protected area, deemed it relevant that the detectaphone’s use occasioned no physical trespass.\textsuperscript{51} The \textit{Goldman} Court found “no reasonable or logical distinction” between what agents did in this case and what they had done in \textit{Olmstead}.\textsuperscript{52}

The physical trespass test for a Fourth Amendment search reached its logical extreme in \textit{Silverman v. United States}.\textsuperscript{53} In \textit{Silverman}, a microphone was inserted under a baseboard until it made contact with the heating duct that ran through the entire house, creating a perfect sounding board through which conversations could be overheard.\textsuperscript{54} However, the Court’s ruling did not pivot on the officers’ ability to hear the entire conversation, but instead upon the microphone’s physical intrusion. The \textit{Silverman} Court, while avoiding “the technicality of a trespass upon a party wall as a matter of local [property] law,” concluded that a search occurred due to an “unauthorized physical penetration into the premises,” which it labeled a “constitutionally protected area.”\textsuperscript{55}

By focusing on the tangible boundaries of walls enclosing constitutionally protected areas, the Court strayed from the Fourth Amendment’s core value of privacy. After all, one would assume that the invasion that truly bothered Mr. Silverman was the government’s eavesdropping upon the content of his conversation, not its physical penetration of his party wall. Therefore, the Court ultimately turned away from its physical trespass precedent in favor of a new standard based on reasonable expectation of privacy.

This fundamental change occurred in \textit{Katz v. United States}.\textsuperscript{56} In \textit{Katz}, federal agents attached an electronic listening device to a phone booth \textit{Katz} frequently used to transmit gambling information.\textsuperscript{57} In the resulting prosecution, the parties dutifully relied upon the physical trespass case law in litigating the suppression motion; however, the Court in \textit{Katz} responded by

\begin{itemize}
\item \textsuperscript{51} See \textit{id.} at 135.
\item \textsuperscript{52} See \textit{id.}
\item \textsuperscript{53} 365 U.S. 505 (1961).
\item \textsuperscript{54} See \textit{id.} at 509-10.
\item \textsuperscript{55} \textit{Id.}
\item \textsuperscript{56} 389 U.S. 347 (1967).
\item \textsuperscript{57} See \textit{id.} at 348.
\end{itemize}
ridiculing the "physical penetration" approach, declaring that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'" Justice Stewart, writing for the Court, then rubbed salt in the wounds by stating the obvious: "[T]he Fourth Amendment protects people, not places."

Justice Harlan, in his concurring opinion, actually crafted the current definition of a Fourth Amendment search as a government intrusion upon privacy expectations. Specifically, he wrote: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Justice Harlan's articulation of a Fourth Amendment search as an intrusion on genuine and legitimate privacy expectations has survived to this day. Therefore, it is crucial, in weighing the Fourth Amendment privacy issue implicated by the Pentium III chip, to explore how the PSN could potentially affect society's view of what is a reasonable expectation of privacy.

B. The Impact of Private Conduct on the Scope of the Fourth Amendment

At first blush, it seems curious that Intel, a commercial business with no governmental role or responsibility, could alter the boundaries of a right guaranteed by the United States Constitution. However, under the current definition of a Fourth Amendment search, private persons, in their daily activities, not only can but invariably do affect what the Court will recognize as an intrusion on a reasonable expectation of privacy.

The Court recognized as much in Katz. Justice Stewart took care to specify the details needed to secure privacy in a conversation in a phone booth, noting that "[o]ne who occupies it, shuts the door behind him, and pays a toll that permits him to place a call is surely entitled to assume that the words he

58. Id. at 350-51.
59. Id. at 351-52.
60. See id. at 381 (Harlan, J., concurring).
61. Id.
utters into the mouthpiece will not be broadcast to the world.”\textsuperscript{62}

The \textit{Katz} Court, in premising its conclusion on privacy expectations with particulars of individual conduct, created a connection between its newly crafted “reasonable expectation of privacy” standard and individual behavior. Justice Stewart then made the link between private conduct and constitutional boundaries explicit: “To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”\textsuperscript{63}

In \textit{United States v. White},\textsuperscript{64} the Court recognized that not only could an individual affect the boundaries of his own Fourth Amendment privacy rights, but third parties could as well. In \textit{White}, as part of a narcotics investigation, an informant wearing a concealed radio transmitter had several conversations with the defendant.\textsuperscript{65} The informant, Harvey Jackson, thus electronically gathered evidence against the defendant while the two spoke at various locations, including Jackson’s home and car and the defendant’s home.\textsuperscript{66}

The Court in \textit{White} noted that it had already determined, in the pre-\textit{Katz} case of \textit{Hoffa v. United States},\textsuperscript{67} that communications to a trusted colleague who turns out to be a government informant are not protected by the Fourth Amendment.\textsuperscript{68} The \textit{White} court re-articulated \textit{Hoffa’s} conclusion in line with \textit{Katz}’s “reasonable expectation of privacy” logic.\textsuperscript{69} The \textit{White} Court recognized that a defendant has a subjective privacy expectation when confiding in a criminal colleague, otherwise the conversation would never occur.\textsuperscript{70} However, the expectation was not objectively reasonable because “one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But, if he has no doubts, or allays them, or risks

\begin{itemize}
\item \textit{Katz}, 389 U.S. at 352 (emphasis added).
\item \textit{Id.}
\item 401 U.S. 745 (1971).
\item \textit{See id. at} 746-47.
\item \textit{See id. at} 747.
\item 385 U.S. 293 (1966).
\item \textit{See White}, 401 U.S. at 749.
\item \textit{See id. at} 751-52.
\item \textit{See id.}
\end{itemize}
what doubt he has, the risk is his.” 71 Thus, assuming the risk and speaking to the companion undermines the reasonableness of the privacy expectation. Of course, the “third party” in White was an individual who related conversations to the government, and therefore was himself a government agent.

The next step, that of having the Fourth Amendment’s boundaries affected by private parties separated from the government, was demonstrated in Smith v. Maryland.72 In Smith, the defendant robbed Patricia McDonough and after the robbery, harassed McDonough with “threatening and obscene phone calls.”73 One time the caller told McDonough to step out on her front porch, and when McDonough did so, she saw the car previously involved in the robbery “moving slowly past her home.”74 Police traced the car’s license plate to the defendant and had the telephone company install a pen register to record the numbers dialed from his home.75 The next time a call was placed from the defendant’s home to the victim’s, the pen register revealed the simple fact that a call was placed from the defendant’s number to the victim’s number.76 This ultimately led to the defendant’s arrest and conviction for robbery.77

It would be difficult to overstate the importance of Katz’s “reasonable expectation of privacy” test in Smith. Justice Blackmun, writing for the Smith Court, acknowledged that to determine “whether a particular form of government-initiated electronic surveillance is a ‘search’ within the meaning of the Fourth Amendment, our lodestar is Katz v. United States.”78 In applying the Katz standard to the facts in Smith, the Court paid particular attention to private parties’ actions and assumptions, whether they are the phone companies or the callers themselves.79 After identifying the pen register’s “limited capabilities,” (this device discloses “only the telephone numbers

71. Id. at 752.
73. See id. at 737.
74. See id.
75. See id.
76. See id.
77. See id. at 737-38.
78. Id. at 739.
79. See id. at 741-42.
that have been dialed” rather than conversations), Justice Blackmun considered the expectations of telephone users and expressed doubt that individuals expected the numbers they dialed to remain private. He surmised: “[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through the telephone company switching equipment that their calls are completed.”

The Smith Court then considered expectations in light of actions by private third parties, such as phone companies. Here, Justice Blackmun continued:

All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies “for the purposes of checking billing operations, detecting fraud, and preventing violations of the law.”

The Smith Court went still further in assessing the conduct of private parties regarding this surveillance technique. Phone companies used pen registers to track all calls “subject to a special rate structure,” and were “regularly employed ‘to determine whether a home phone is being used to conduct a business, to check for a defective dial, or to check for overbilling.’” The cumulative impact of these private activities led the Court to conclude: “[I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.” Hence, Smith offered an explicit example in which the Court measured the Fourth Amendment right to privacy by the yardstick of private actions.

The influence of a private person’s intrusions on constitutionally-protected privacy might have reached its logical
extreme in *California v. Greenwood*. In *Greenwood*, Laguna Police Department Investigator Jenny Stracner investigated a tip that the defendant might be involved in narcotics trafficking. As part of her investigation, Stracner asked the trash collector to give her Greenwood’s trash without mixing it with garbage from other houses. She then searched the trash for evidence of drug use or trafficking. The evidence she collected supported a warrant to search Greenwood’s home. This activity presented the question whether a government intrusion into a person’s trash on the curb constituted an intrusion on an expectation of privacy that “society is prepared to accept . . . as reasonable.”

The *Greenwood* Court’s conclusion that society was not prepared to find a reasonable expectation of privacy in trash left on the curb was based on actions by all sorts of individuals other than government officials. Justice White, writing for the *Greenwood* Court, declared: “It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoopers, and other members of the public.” The implications of this line of reasoning are startling. The Fourth Amendment’s boundaries, based on the Court’s list of potential intruders, can be diminished by wrongdoers (“snoopers”), persons too young even to vote (“children”), and even individuals with four legs (“animals”). If the neighborhood cat or dog can undermine the reasonableness of privacy expectations, it would certainly seem plausible that a powerful corporation like Intel can do the same.

**C. Equating the Ability To Frustrate Reasonable Expectations of Privacy with the Lack of Any Protected Privacy**

When considering inroads on privacy, the Court has often employed the worst case scenario as its standard. The *Greenwood* case again provides a dramatic example. In support

---

87. See id. at 37.
88. See id.
89. See id. at 37-38.
90. Id. at 40.
91. See id.
92. Id.
93. See id.
of its assertion that trash is vulnerable to "animals, children, scavengers, [and] snoops," the Court cited numerous examples of "Murphy's Law." Justice White used the case of *North Dakota v. Ronngren* to illustrate canines' threat to privacy. In *Ronngren*, a dog dragged the defendant's garbage into his neighbor's yard, and the neighbor allowed the police to search the bag. Thus, the Court relied upon an extreme example of a canine overachiever. There, the dog not only intruded upon the trash but also delivered it to a neighbor who provided consent to a police search. Yet, Justice White went on to top the delivery dog with a consumer columnist story: "the 'Rich Lady' from Westmont who once a week puts on rubber gloves and hip boots and wades into the town garbage dump looking for labels and other proofs of purchase" needed to obtain manufacturer's refunds. In relating this event, the *Greenwood* Court seemed to miss the crucial point that this story came from a newspaper column. Columnists write about such items because they are remarkable, and thus the very stuff of curiosity and news.

The *Greenwood* Court's confusion of life's rare exceptions to the usual rules was illustrated by its next example, that "a reporter for a weekly tabloid seized five bags of garbage from the sidewalk outside the home of Secretary of State Henry Kissinger." Did the Court really mean to equate press interest in Henry Kissinger, Secretary of State, Washington D.C. socialite, author, and Nobel Peace Prize winner, with the ordinary citizen? This logic would allow police to peer into our homes and private ceremonies just because the paparazzi have likewise intruded on such celebrities as the Windsors and the Kennedys.

Treating the worst case scenario as if it were the norm has extended beyond garbage collection. In *Florida v. Riley*; the Court trimmed Fourth Amendment privacy in the context of

---

94. *See id.*
95. 361 N.W.2d 224 (N.D. 1985).
96. *See Greenwood*, 486 U.S. at 49 n.2.
97. *See id.*
98. *Id.* at 40 n.3.
99. Justice White wrote that the source of this tale was a "nationally syndicated consumer columnist." *Id.*
100. *Id.* at 40 n.4.
aerial surveillance. In *Riley*, the Pasco County Sheriff's office received a tip that the defendant was growing marijuana on his five acres of rural property. Riley was actually growing the marijuana in a greenhouse located about ten to twenty feet from his mobile home on the property. The greenhouse was enclosed on two sides, with the other two sides covered by trees and shrubs. Further, the greenhouse was covered with corrugated roofing panels and surrounded by a fence bearing "DO NOT ENTER" signs. However, some ten percent of the greenhouse's roof had a hole in it due to missing panels. When an officer following up on the tip learned that he could not see the greenhouse's contents from the public road, he circled 400 feet over respondent's property in a helicopter, and as he looked through the roof's holes and the greenhouse's sides, he saw marijuana growing within. This observation led to a search warrant, search, recovery of marijuana, and formal charges for possession of marijuana.

Justice White, writing the Court's opinion, equated *Riley* with *California v. Ciraolo*, a case in which police made a naked-eye observation of marijuana in a backyard from a fixed-wing aircraft at 1000 feet. The *Ciraolo* Court recognized that the plane's aerial surveillance included the house's curtilage, an area near the house typically sharing the home's Fourth Amendment protections. *Ciraolo* also acknowledged that the

102. *See id.* at 448.
103. *See id.*
104. *See id.*
105. *See id.*
106. *See id.*
107. *See id.*
108. *See id.*
109. *See id.* at 448-49.
111. *See id.* at 208.
112. *See id.* The Supreme Court has acknowledged the common law's historic respect for curtilage as an area deserving the protection of Fourth Amendment privacy. *See* Oliver v. United States, 468 U.S. 170, 180 (1984). The Court in *Oliver* noted:

[The common law distinguished "open fields" from the "curtilage," the land immediately surrounding and associated with the home . . . . The distinction implies that only the curtilage, not the neighboring open fields, warrants the Fourth Amendment protections that attach to the home. At common law, the curtilage is the area to which extends the intimate activity associated with the "sanctity of a man's home and the privacies of life," . . . and therefore has been considered part of the home itself for Fourth
officer's view from the air intruded upon the defendant's subjective privacy expectation because a fence shielded the yard from observation from the street.\textsuperscript{113} Despite these privacy considerations, the \textit{Ciraco}lo Court held that the defendant's privacy expectations from overflights was "unreasonable and [was] not an expectation that society is prepared to honor."\textsuperscript{114}

\textit{Ciraco}lo arrived at this conclusion through the following steps in reasoning. Generally, police are permitted to observe what may be seen "from a public vantage point where [they have] a right to be . . ."\textsuperscript{115} And, like the public, police have been allowed to observe the backyard from the street if their view is unobstructed.\textsuperscript{116} If free to observe the yard from the ground, "[t]hey were likewise free to inspect the yard from the vantage point of an aircraft flying in navigable airspace as this plane was."\textsuperscript{117} The \textit{Ciraco}lo Court concluded:

In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet. The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.\textsuperscript{118}

Thus, the chance that an airline passenger might recognize marijuana plants in the backyard of an anonymous mass of houses enabled officers to pinpoint a particular yard, even if within the home's curtilage, and subject it to repeated fly-overs without triggering the protection of the Fourth Amendment.

The Court in \textit{Riley} then took \textit{Ciraco}lo's logic a step further, or in practical terms, lower. The \textit{Riley} Court consulted Federal Aviation Administration regulations in lowering the Fourth Amendment purposes. Thus, courts have extended Fourth Amendment protection to the curtilage . . . .

\textit{Id.}

\textsuperscript{113} \textit{See Ciraco}lo, 478 U.S. at 209.

\textsuperscript{114} \textit{Id. at 214}.

\textsuperscript{115} \textit{Id. at 213}.

\textsuperscript{116} \textit{See id. at 213}.

\textsuperscript{117} \textit{Id.}

\textsuperscript{118} \textit{Id. at 215}.
Amendment floor for aerial surveillance from 1000 to 400 feet.\textsuperscript{119} In effect, the lowest level of “navigable airspace” came to define the boundary of Fourth Amendment protection, for “[a]ny member of the public could legally have been flying over Riley’s property in a helicopter at the altitude of 400 feet and could have observed Riley’s greenhouse.”\textsuperscript{120} Although the \textit{Riley} Court took care to state that not every observation from navigable airspace “will always pass muster,” it undercut this caveat with its next sentence:

But it is of obvious importance that the helicopter in this case was \textit{not} violating the law, and there is nothing in the record or before us to suggest that helicopters flying at 400 feet are sufficiently rare in this country to lend substance to respondent’s claim that he reasonably anticipated that his greenhouse would not be subject to observation from that altitude.\textsuperscript{121}

The result of this language is an implication that overflights at the FAA minimum are beyond Fourth Amendment inquiry unless the defendant takes on the burden of affirmatively showing special circumstances of privacy.

Thus, when it comes to diminishing Fourth Amendment protection, if it can be done, the Court will always consider it to be done. Once a dog invades one trash can, once the press rummages through a high government official’s rubbish, once an airplane makes an observation at 1000 feet and a helicopter does so at 400 feet, Fourth Amendment protection of these areas forever ceases to exist.

\textbf{III. INTEL’S EFFECT ON THE SCOPE OF FOURTH AMENDMENT PRIVACY}

Intel designed its product, the Pentium III chip, to create the new standard in computing. In this regard, Intel has apparently hit its target. One reviewer, Michael J. Himowitz, compared using the Pentium III to driving a sports car.\textsuperscript{122} He glowingly

\textsuperscript{119} See \textit{Riley}, 488 U.S. at 450.
\textsuperscript{120} \textit{Id.} at 451.
\textsuperscript{121} \textit{Id.} at 451-52.
\textsuperscript{122} See Michael J. Himowitz, \textit{The Souped-Up Pentium III Is Speedy, But Don’t Bother Chucking Your Old PC}, \textit{Fortune}, at 158, Apr. 12, 1999, \textit{available at
described its abilities as a "machine [that] worked beautifully, running games with superb detail, inhaling Web pages through [a] cable modem in a flash, and playing full-screen DVD movies with exquisite resolution and house-rattling sound." Further, as the largest chipmaker on the globe, with its Pentium III chips installed in such popular computers as Dells and Compaqs, Intel's sheer volume of sales will make the Pentium III widespread around the world.

The full Fourth Amendment implications of widespread acceptance and use of Intel's 96-bit serial number become clear upon review of the Court's precedent regarding a Fourth Amendment search. Admittedly, Intel is not a government entity. However, as will be seen, its mammoth size and the immense popularity of its chip may alter the scope of Fourth Amendment privacy. The Fourth Amendment's vulnerability to Intel's influence is a product of the Court's "reasonable expectation of privacy" definition of a search, the Court's consideration of private behavior as affecting the boundaries of Fourth Amendment protection, and the Court's acceptance of the worst case scenario as the standard for privacy invasions.

A. The "Reasonable Expectation of Privacy" Rule and Technological Advancements

As previously noted, the Court's current definition of a Fourth Amendment "search" was crafted in the context of advancing technology. When, in Katz, the Court was faced with yet another example of technology empowering official intrusion beyond the concrete boundaries of a house's walls or a phone

http://www.elibrary.com. Mr. Himowitz declared:

Driving a new Pentium III computer is like slipping behind the wheel of a souped-up Porsche. It's great to see the world whiz by, but it's questionable whether you need all this horsepower just to get to the office. Of course, Intel is spending $300 million on TV and print ads to convince you that you can't do without its latest hot-rod microprocessor.

_Id_.

123. _Id_.
124. See Kornblum, _supra_ note 3; Himowitz, _supra_ note 122.
125. See discussion _supra_ Part II.
128. See Katz v. United States, 389 U.S. 347 (1967); see also discussion _supra_ Part II.A.
booth's doors, it finally rejected its own physical trespass upon a "constitutionally protected area" test\textsuperscript{127} as unworkable.\textsuperscript{123}

The Court continued to use technology in defining reasonable expectations of privacy even after \textit{Katz}. Indeed, Fourth Amendment boundaries were further refined in the "beeper" tracking device case, \textit{United States v. Knotts}.\textsuperscript{123} In \textit{Knotts}, police placed a beeper, a "radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver," in a five-gallon drum of chloroform bought by a defendant, Darryl Petschen.\textsuperscript{130} Chloroform is a "precursor" chemical in the manufacture of illegal drugs.\textsuperscript{131} Using the beeper, police were able to track the drum to the defendant's methamphetamine lab in a secluded cabin.\textsuperscript{132}

Justice Rehnquist, writing for the \textit{Knotts} Court, found the use of a beeper unremarkable. "The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways."\textsuperscript{133} Further, driving on public streets was hardly a private activity. Justice Rehnquist noted:

\begin{quote}
A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.\textsuperscript{134}
\end{quote}

\textsuperscript{127} \textit{See} Silverman v. United States, 365 U.S. 505, 509-10 (1961); \textit{see also} discussion supra Part II.A.
\textsuperscript{128} \textit{Katz} deemed the \textit{Olmstead/Goldman} test as "so eroded" as to be "no longer ... controlling." \textit{Katz}, 389 U.S. at 353.
\textsuperscript{129} 460 U.S. 276 (1983).
\textsuperscript{130} \textit{Id. at 277.}
\textsuperscript{131} \textit{Id. at 278.}
\textsuperscript{132} \textit{Id. at 277.}
\textsuperscript{133} \textit{Id. at 281.}
\textsuperscript{134} \textit{Id. at 281-82.}
Moreover, the technological advance of a beeper had no constitutional impact. Justice Rehnquist opined:

The fact that officers in this case relied not only on visual surveillance, but also on the use of a beeper to signal the presence of Petschen’s automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.

*Knotts* therefore added a crucial dimension to the reasonable expectation of privacy calculus. Technology is of no Fourth Amendment significance if its use merely makes more convenient activities that police could have pursued without a helpful new gadget. Conceivably, police could have stationed a multitude of unmarked cars in the area around the chloroform manufacturer in anticipation of every possible route to the drug lab. Instead, law enforcement achieved the same result with far fewer officers by employing a tracking device.

This reasoning suffers two blind spots. First, limits on police resources may be impractical to employ many officers for one drum of chloroform. Second, figuring that motorists and pedestrians will take note of a car’s speed and direction in order to avoid a collision, or to take a passing interest in its color or style, is far different from assuming that one is being followed. To require citizens to reasonably expect that they are being followed is to elevate the *Katz* standard to paranoia.

*Knotts’* interpretation of *Katz* has ominous implications for Pentium III users. All sorts of groups are busy attracting computer users to the Internet, and no segment of society seems untouched. Companies, whether they sell books, music, toys, clothes, or desserts, offer customers the ability to purchase goods online. Those on the Internet may also seek advice in a dizzying variety of topics, including stocks, higher education, addiction, taxes, and health. The Internet also acts as a

135. *See id.* at 282.
136. *Id.*
gathering place for those of similar interests or beliefs, whether they are hobbyists, political activists, or religious worshipers. 139

Conceivably, the Court could analogize the PSN to the Knotts’ beeper. People could recognize an individual as he or she shopped at a particular store or attended certain meetings or gatherings. Since such actions would be vulnerable to public notice, police could likewise learn all the details of one’s comings and goings. In fact, officials could seek informants in various industries or place agents undercover at corporations, organizations, and churches to gather information. Since all the information about an individual’s public acts, such as shopping at a store or visiting a friend, could conceivably be observed by others, the government could collect all this information by investigators on foot without intruding on reasonable expectations of privacy, and thus not trigger the Fourth Amendment. Since the government could watch the public acts of every individual by employing a plethora of police officers, the Court might reason that it could also do so by tracking PSNs. Since in Knotts “police were able to augment... their sensory faculties” 140 without altering the constitutional situation, police might likewise ease their burden by relying on Intel’s PSN, without constitutional consequence.

B. Intel’s Actions May Impact the Court’s “Reasonable Expectation of Privacy” Assessment

Generally, when people seek privacy, they wish to keep something secret from all others, whether those “others” are the government or the public at large. When a person makes a call from a home phone, he or she would be offended by any eavesdropping, whether carried out by a police officer or a neighbor. This seems to be the assumption guiding the Court’s reasonable expectation of privacy jurisprudence. In Katz, a toll paid for privacy was against all the world, not just the official world. 141 In White, the Court concluded that the defendant

140. Knotts, 460 U.S. at 282.
141. See Katz, 389 U.S. at 352.
assumed a risk to his privacy by sharing his guilty secret with a companion.\textsuperscript{142} This conclusion was not altered by the fact that White’s confederate turned out to be acting as a government informant.\textsuperscript{143} Further, in \textit{Smith} the Court found that the conveyance of phone numbers to private third parties destroyed “\textit{any} expectation that the numbers they dial will remain secret.”\textsuperscript{144} Thus, sharing numbers with the operator was the equivalent of sharing it with everyone, including the government. Therefore, collection of those numbers in a criminal investigation fell outside of Fourth Amendment protection.\textsuperscript{145} Perhaps the equation between private and official intrusion reached its logical limit in \textit{Greenwood}, where a dog enabled government intrusion; if dogs can go through trash, so can the government.\textsuperscript{146}

Since a phone company, a neighborhood snoop, or a dog can influence the boundaries of the Fourth Amendment, certainly one of Silicon Valley’s most successful companies can similarly impact the scope of Fourth Amendment protection. This is even more likely due to the sheer size of the Pentium III marketplace. Instead of one reporter digging through Henry Kissinger’s trash, Intel has produced millions of chips, approximately ninety percent of the personal computer market,\textsuperscript{147} which can be used to allow new invasions with each visit to a Web site. The aggregate impact on an Internet user’s reasonable expectation of privacy is therefore enormous. With millions of computer users assuming the risk of a hacker surreptitiously obtaining their PSNs, no individual user could reasonably expect privacy in the use of his or her computer equipped with the Pentium III processor.

\textbf{C. Intel’s PSN Will Undermine Any Reasonable Expectation of Privacy on the Internet}

If the Court were to adopt a slogan for its reasonable expectation of privacy rule, it might be: “If a privacy invasion

\textsuperscript{142} \textit{See United States v. White}, 401 U.S. 745, 752 (1971).
\textsuperscript{143} \textit{See id.}
\textsuperscript{144} \textit{Smith v. Maryland}, 442 U.S. 735, 743 (1979) (emphasis added).
\textsuperscript{145} \textit{See id.}
\textsuperscript{147} \textit{See Latest Intel Chip, supra} note 1.
can be done without physical invasion, consider it done.” If a neighborhood dog invaded trash on the curb, then all trash on every curb is considered equally vulnerable.\textsuperscript{148} If the press could scrounge through Henry Kissinger’s trash, then everyone’s trash is fair game.\textsuperscript{149} If FAA regulations enabled a helicopter to get a peek through ten percent of a roof on a greenhouse,\textsuperscript{150} it is unreasonable to consider the area, even if within curtilage, as private from public view.\textsuperscript{151} 

Thus, if Zero-Knowledge Systems could send a “Trojan horse” into a Pentium III computer to bypass Intel’s utility, thus making the “serial number available even when Intel’s utility says the feature has been turned off,”\textsuperscript{152} then it would be unreasonable to ever assume that the PSN is private. The undermining of the reasonable expectation of privacy in the serial number would persist, despite the existence of later patches.\textsuperscript{153} Since Intel’s PSN is permanently embedded into the chip during the manufacturing process\textsuperscript{154} and the blocking utility is merely software which “can be attacked . . . with enough time and effort,”\textsuperscript{155} no utility can solve privacy concerns once and for all. Therefore, reliance upon Intel’s corrective utility does not seem to create a privacy expectation worthy of Fourth Amendment protection. Indeed, we must presume that all Internet transactions, whether to stores, chat rooms, or special interest sites, are constantly monitored. Thus, the voluntary purchase and use of the Pentium III will function as a forfeiture of the Fourth Amendment right to privacy.

\textsuperscript{148} See Greenwood, 488 U.S. at 40 n.2.
\textsuperscript{149} See id. at 40 n.4.
\textsuperscript{151} See id. at 450.
\textsuperscript{152} See Menefee, supra note 9.
\textsuperscript{153} For example, although Symantec Corp. has blocked a Zero-Knowledge Systems’ crack of Intel’s Pentium III serial number blocking utility, the security concerns about the utility software still prevail. See supra notes 27-30 and accompanying text. Id.
\textsuperscript{154} See PSN Q & A, supra note 4.
\textsuperscript{155} See id.
CONCLUSION

If it is true that “[t]he road to Hell is paved with good intentions,”\textsuperscript{156} then perhaps the paving stones are Pentium III chips. Intel's aims in creating the PSN for its new chip were seemingly noble: Intel considered its PSN as a “security feature” which would “enhance [customers’] Internet experience.”\textsuperscript{157} The Pentium III was meant to make cyber life easier by “authenticating participants in a secure chat room” and “enhanc[ing] security in e-commerce situations.”\textsuperscript{158} To witness Intel’s pride in preserving people’s privacy, one need only review the chipmaker’s “Online Privacy Policy.”\textsuperscript{159}

It is therefore ironic that a company concerned with online privacy might have, in the very effort to limit intrusion into computer users’ lives, created a device that diminishes the scope of privacy protection under the Fourth Amendment. Indeed, the Pentium III microchip initially seems ill-equipped to diminish the scope of the Fourth Amendment. Intel’s computer users probably subjectively expect their processor serial numbers to remain secret despite the concerns raised by privacy groups and Trojan horses. Further, Intel exerts no official power in determining the scope of constitutional rights. Finally, even if organizations like Zero-Knowledge Systems can temporarily access the PSN, it can be assumed that Intel will remain vigilant in patching holes in its software utility. Yet all of these facts offer no solace, for each has been effectively neutralized by the Court’s case law.

\textsuperscript{156} JOHN RAY, ENGLISH PROVERBS (1870), reprinted in BARTLETT'S FAMILIAR QUOTATIONS 136 n.8 (Emily Morison Beck ed., Little, Brown & Co. 1980) (1855).

\textsuperscript{157} See PSN Overview, supra note 6.

\textsuperscript{158} Id.

\textsuperscript{159} “Intel respects your privacy choices. If you give us personal information, we will treat it according to this policy . . . . We will not change the way in which we use your personal information without your consent.” Intel's Online Privacy Policy, Intel Support Forum, arhttp://support.intel.com/sites/corporate/privacy.htm (last visited Aug. 23, 2000). Intel backs up this policy by allowing visitors to its Web sites to “remain anonymous,” by explaining how the company will use any personal information that is requested, by refusing to provide any personal information to other companies without permission, and by using encryption for “sensitive information” such as credit card numbers. See id.
The Pentium III’s corrosive effect on Fourth Amendment privacy comes as a result of a combination of Court cases.\textsuperscript{163} Katz limited Fourth Amendment protection only to invasions on privacy expectations that society itself is prepared to recognize as reasonable. Greenwood deemed that such expectations could be undermined by individuals outside of the government and, for that matter, outside of the human species. Finally, the logic of cases such as Cirillo and Riley have made the Fourth Amendment’s protection against unreasonable searches the Humpty Dumpty of the Bill of Rights; once a reasonable expectation of privacy in a particular case is invaded, it forever remains unreasonable to rely on privacy in that context. Thus, once broken by the Pentium III’s serial number, Fourth Amendment privacy can never be put back together again.

\begin{flushright}
160. See discussion \textit{supra} Parts II-III.
\end{flushright}