Journal of Law and Policy

Volume 14
Issue 1
SCIENCE FOR JUDGES V:
Risk Assessment Data: Disclosure and Protection

Article 9

2005

Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data

Susan W. Brenner

Leo L. Clarke

FOURTH AMENDMENT PROTECTION FOR SHARED PRIVACY RIGHTS IN STORED TRANSACTIONAL DATA

Susan W. Brenner & Leo L. Clarke[*]

INTRODUCTION

We live in a world of pervasive, ubiquitous data collection and retention.[1] Modern computer technology permits us to acquire and retain knowledge, communicate instantly and globally, purchase goods and services, engage in hobbies, and participate in politics and cultural affairs, all in less time and with less expense than once dreamed possible. One major effect of this revolution has been a serious reduction in an individual's rights and expectations of

---

[*] Susan W. Brenner is the NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law. Leo L. Clarke is an Associate Professor at the Thomas M. Cooley Law School.

[1] The phrases "ubiquitous technology" and "ubiquitous computing" are used interchangeably to refer to technologies woven into the fabric of everyday life. *See*, *e.g.*, Niall Winters, *Personal Privacy and Popular Ubiquitous Technology*, UBICONF (2004), http://www.uclic.ucl.ac.uk/projects/ubiconf/materials/Papers/Niall%20Winters.pdf. "Ubiquitous computing involves having computing devices essentially everywhere in the home, office or public area, as well as easy, natural ways for people to interact with them. Wireless technologies, sensors, radio frequency identification (RFID) tags and machine-to-machine communications will play a big role in this new area of computing." John Blau, *German Group Studies Ubiquitous Computing, Data Privacy*, NETWORK WORLD, Dec. 22, 2004, http://www.nwfusion.com/news/2004/1222germagroup.html. This article focuses on "communicative" technologies instead of, say, industrial or agricultural technologies. Its concern is with technologies that can be used to generate information, collect information and/or share information. *See infra* Part I. The Fourth Amendment is, of course, concerned with channeling how law enforcement finds (searches) and obtains (seizes) varieties of information. *See infra* Part II.A.

privacy. It has become increasingly common for data about our transactions and ourselves (Data) to be collected and retained by third parties (Collectors) who often disclose more intimate details of our lives and lifestyles than would have ever been imaginable or acceptable just a decade ago. In turn, this retention creates an unprecedented risk that a local, state or federal government (Government) can obtain, without the need for a warrant, Data about individuals (Consumers) to which it has never had access.[2] This risk arises because a Collector in possession of Data could decide to disclose that Data to law enforcement officials, and under certain United States Supreme Court decisions, the Consumer to whom the Data relates could be deemed to have assumed the risk of that disclosure.[3]

---

[2] In 2004, the Pew Internet & American Life Project surveyed "1,286 Internet stakeholders" to elicit their views as to how the Internet will change our lives between 2004 and 2014. ELON UNIVERSITY, PEW INTERNET & AMERICAN LIFE PROJECT, THE EXPERTS SURVEY, IMAGINING THE INTERNET (2004), http://www.elon.edu/predictions/q12.aspx. One statement as to which the survey requested reactions was:

> As computing devices become embedded in everything from clothes to appliances to cars to phones, these networked devices will allow greater surveillance by governments and businesses. By 2014, there will be increasing numbers of arrests based on this kind of surveillance by democratic governments as well as by authoritarian regimes.

Id. Among the responses was the following: "We must think through the way technology changes what is private, and develop new concepts of reasonable privacy that preserve liberty and are workable in a networked world." *Id.*

[3] It appears that the United States Department of Justice may be considering "the explosive idea" of requiring, presumably through legislation, Internet Service Providers (ISPs) to retain records of all e-mail and web browsing activities by customers. Declan McCullagh, *Your ISP as Net Watchdog*, CNET NEWS, June 16, 2005, http://news.com.com/Your+ISP+as+Net+watchdog/2100-1028_3-5748649.html. A requirement that records be retained can only indicate a strong Government interest in the types of requests under consideration in this article. At the present time, the Stored Wire and Electronic Communication Transaction Records Act requires ISPs to retain certain transactional records for 90 days only upon Government request and to produce those records under certain conditions which are consistent with Fourth Amendment protections. 18 U.S.C. § 2703 (2005). That statute is not germane to our discussion because nothing under that statute precludes an ISP from

Privacy evolved as a "bricks and mortar" concept.[4] When the Fourth Amendment was added to the Constitution, the real-world was the *only* world; technology had not yet given us the ability to transcend the strictures of the real-world.[5] We now have that ability: we can substitute the virtual realities provided by computer technology for the physical world; we can communicate instantaneously with almost anyone from almost anywhere and we use technologies to make our lives easier, to earn our living and even for our own amusement.

Our use of this technology has resulted in the creation of new relationships whereby we now use third parties to process or store information that we previously maintained ourselves. We are also replacing inefficient real-world relationships that have become too expensive, too slow or too imprecise. While these changes may enhance convenience and cost-saving efficiency, they do so at the expense of privacy. For example, many Internet users now rely on third-party providers for the digital storage of private documents, correspondence (including e-mail), business and financial records, family photographs and hobby information. Do we lose our privacy interest in those materials when we entrust them to a third party? In the past, when information was disclosed to educational, religious and medical institutions it was done either orally or in scattered paper documents. Now, such information is stored in a digital format allowing that information to be collected, sorted and reported in ways never before possible. With the increasing computerization of home services, from home security services and cable television to "smart houses,"[6] security information that

---

voluntarily disclosing information to Government without requiring Government to comply with the Act.

[4] The phrase "bricks-and-mortar" "[d]escribes a site that has a physical presence in the real world (as opposed to a virtual presence in the online world)." THE WORD SPY (2005), http://www.wordspy.com/words/bricks-and-mortar.asp.

[5] NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 79–105 (1937).

[6] "Smart houses" (or "aware homes") incorporate intelligent, embedded systems which interact with the occupants and with outside systems. *See*, *e.g.*, GEORGIA INSTITUTE OF TECHNOLOGY, THE AWARE HOME, http://www.cc.

was previously available only to family members is now communicated to databases managed by third parties. The increasing sophistication of remote sensing and database technology means that the amount of information available to providers of utility and telecommunications services has dramatically increased. Do we lose our privacy interest in that information because it is now more efficient to collect it in a database where it can be searched and sorted in a myriad of ways?

This discussion brings us to the question at hand: Can the Fourth Amendment's privacy guarantee be adapted to deal with a world in which technology is increasingly pervasive—a world of ubiquitous technology?[7] In this article, we consider whether Fourth Amendment protections should apply to Data provided by a Consumer to a Collector pursuant to a confidentiality agreement when the Data would not otherwise be available to Government without a warrant or proof that an exception to the warrant requirement applies. Our contention is that Fourth Amendment protection should not vanish simply because advances in technology permit, and to a certain extent make unavoidable, massive Data collection and mining that expose Consumers to the enhanced risks of a Collector's breach of trust.[8] Instead, we argue

---

gatech.edu/fce/ahri/ [hereinafter THE AWARE HOME]; PHILIPS RESEARCH, AMBIENT INTELLIGENCE: A NEW USER EXPERIENCE, http://www.research.philips.com/InformationCenter/Global/FArticleSummary.asp?lNodeId=712 [hereinafter AMBIENT INTELLIGENCE]. *See also* Mark Ward, *Smart Homes Offer A Helping Hand,* BBC NEWS (May 19, 2004), http://news.bbc.co.uk/1/hi/technology/ 3715927.stm. An "aware home" will "be able to recognize the people that live in it, adapt . . . to them [and] learn from their behavior." AMBIENT INTELLIGENCE, *supra.* Similar systems will become features of offices, hotel rooms and other environments. *See*, *e.g.*, K. DUCATEL ET AL., EUROPEAN COMM'N, IST ADVISORY GROUP, SCENARIOS FOR AMBIENT INTELLIGENCE IN 2010, 4-7, (February 2001), *available at* http://www.newscenter.philips.com/assets/Downloadablefile//ISTAG_scenarios-31461215.pdf [hereinafter EUROPEAN COMMISSION, SCENARIOS FOR AMBIENT INTELLIGENCE].

[7] *See*, *e.g.*, Winters, *supra* note 1; Blau, *supra* note 1.

[8] Data encryption technologies could be employed to eliminate the risk of Government access. However, reliance on encryption would not eliminate the need for Fourth Amendment protection for several reasons. First, Consumers are

that protection of such Data is mandated by the doctrine of *Katz v. United States*,[9] which held that the Fourth Amendment protects information as to which the individual has exhibited a subjective expectation of privacy as long as the expectation is one that society recognizes as reasonable. In other words, we argue that the Fourth Amendment should not permit Government to reap a windfall from a Collector's maintenance of confidential information relating to its transactions with Consumers.

We begin, in Section I, by demonstrating the need for what we term "relation-based shared privacy." We briefly explain how under the Constitution, the societal benefits of pervasive, ubiquitous technology can only be achieved if we recognize the privacy of certain stored transactional data. In the absence of a constitutional recognition of that privacy, the only alternatives are to forego utilization of the technology or to resort to inefficient barriers to exploitation of privacy.

Section II(A) explains how relation-based shared privacy is consistent with a long history of Fourth Amendment jurisprudence relating to, and dealing with, technological advances. Section II(B) then demonstrates how the Supreme Court's post-*Katz* pronouncements about consent and assumption of risk are inconsistent with that history and the recognition of a privacy interest in transactional data.

In Section III, we describe in more detail the contours of relation-based shared privacy. We define the nature of the required relationship between Consumer and Collector and the criteria Data must meet to receive Fourth Amendment protection. Essentially, the Consumer is entitled to Fourth Amendment protection for Data

---

unlikely to undertake encryption of their own accord, if only because current encryption techniques are difficult to use, at least for those who do not have some technical expertise. Second, encryption would lead to its own inefficiencies because uniform standards of encryption do not yet exist. As a result, encryption would reduce the benefits of pervasive technology to the extent it would interfere with the ability to gather and mine data obtained at various times and from various sources for commercial and other purposes. Finally, there is no reason to believe that Government could not obtain from the Collector the necessary key(s) to the encrypted data.

[9] 389 U.S. 347 (1967). For more on *Katz*, see *infra* Part II.A.

maintained by a Collector pursuant to a confidentiality agreement and with whom the Collector has a "trust-based" relationship (with "trust-based" defined broadly and not legally), as long as the Data is maintained at least in part for the Consumer's benefit and is directly accessible by the Consumer. We conclude that, if those conditions are satisfied, Government should not be able to obtain the Data merely upon request to the Collector, absent proof that Government could otherwise have obtained the Data through use of its ordinary procedures in the course of a good faith investigation of a crime.

I. THE NEED FOR PRIVACY IN AN ERA OF UBIQUITOUS INFORMATION TECHNOLOGY

> *Recent inventions and business methods call attention to the next step which must be taken . . . for securing to the individual what Judge Cooley calls the right 'to be let alone.'*[10]

---

[10] Samuel Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 195 (1890), *available at* http://www.louisville.edu/library/law/brandeis/privacy.html (quoting THOMAS M. COOLEY, THE LAW OF TORTS 29 (2d ed. 1888)) [hereinafter Warren & Brandeis]. The Fourth Amendment offered no protection from these activities because it only applies to state action. *See*, *e.g.*, Poe v. Ullman, 367 U.S. 497, 549 (1961). The "evils" Warren and Brandeis were addressing resulted from the efforts of private citizens, which is why they ultimately cast their right to privacy as a tort: those whose privacy was violated could bring an "action of tort for damages in all cases" and could seek an injunction in "a very limited class of cases." Warren & Brandeis, *supra* at 219. This aspect of the Warren-Brandeis right is relevant to the present discussion because it represents an early attempt to deal with the impact technology has upon "informational privacy," i.e., with an individual's ability to exercise some control over how the private sector gathers, disseminates and uses personal information. *See*, *e.g.,* Winters, *supra* note 1 (explaining informational privacy as the ability of "'individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others'") (quoting ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967) [hereinafter WESTIN, PRIVACY AND FREEDOM]). *See also* Alan F. Westin, *Social and Political Dimensions of Privacy,* 59 J. OF SOC. ISSUES 431, 431 (2003) [hereinafter Westin, *Social and Political Dimensions*] (explaining privacy as "the claim of an individual to

In 1890, Samuel Warren and Louis Brandeis published their famous article, *The Right to Privacy*,[11] which argued for a common law cause of action for invasion of an individual's privacy. This differed from the contemporaneous Fourth Amendment concept of privacy because the common law cause of action (i) was directed at private parties and (ii) did not involve a zero-sum approach to privacy.[12] The article is of interest here for two reasons. First, it was an early recognition of the changing notion of privacy in our society, especially in light of technological advances such as photography, newspaper publishing and the interception of telephone communications.[13] Second, and more importantly, it represents an early attempt to deal with the impact technology has upon "informational privacy."[14] Warren and Brandeis

---

determine what information about himself or herself should be known to others . . . . This, also, involves . . . what uses will be made of it by others"). *See generally* Ken Gormley, *One Hundred Years of Privacy,* 1992 WIS. L. REV. 1335, 1350 (1992).

[11] Warren & Brandeis, *supra* note 10, at 193.

[12] *Id*. As is explained later in the text, the Fourth Amendment has historically been interpreted as incorporating a zero-sum conception of privacy. In a zero-sum conception of privacy, only two states exist: private or not-private.

[13] *See infra* note 14. For an extensive analysis of the background and content of the Warren & Brandeis article, see Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, __ MISS. L. J. __ (2005) (forthcoming) [hereinafter Brenner].

[14] Warren and Brandeis were reacting to late nineteenth-century technology: improved printing and photograph reproduction, hand-held cameras, bugs and other eavesdropping devices. These and other technologies transformed personal information into a commodity; the press in prior eras had published information about "notables," but the subjects were usually able to control the information that went to the press. *See*, *e.g.*, MICHAEL SCHUDSON, DISCOVERING THE NEWS: A SOCIAL HISTORY OF AMERICAN NEWSPAPERS 12-57 (1978). *See generally* FREDERICK HUDSON, JOURNALISM IN THE UNITED STATES FROM 1690-1872 (1873). The proliferation of informational technologies and attendant demand for information that arose at the end of the nineteenth century changed all this; the socially- and politically-prominent were obvious targets. *See*, *e.g.*, *id.* at 1352 n.84 (illustrating how the press hounded President Grover Cleveland on his honeymoon). However, just as today, the technology soon affected all segments of the population. *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO

demonstrated that an individual's ability to exercise some control over how the private sector gathers, disseminates and uses personal information is fundamental to an ordered society.[15] Warren and Brandeis faced several conceptual difficulties in articulating their new right to informational privacy. For our purposes, the most fundamental difficulty went to the essence of the principle: What is "private"? The Fourth Amendment has historically been interpreted as incorporating a zero-sum conception of privacy in which only two states exist: private or not-private.[16] However, this simplistic notion did not work for Warren and Brandeis because they were deeply concerned with how new technologies affected traditional understandings of privacy, particularly with regard to the capturing and exploiting of information that was in the public domain, such as photographs and descriptions of the activities of the social or political elite.[17] In this vein, since it was Warren and Brandeis's goal to control the collection, dissemination and use of information about individuals, they sought to redefine "privacy" to make it more consistent with and analogous to a property right.[18] The eventual adoption by virtually every U.S. state of the Warren-Brandeis analysis demonstrates that such a redefinition was an essential consequence of the evolution of these particular

---

THE INTERNET 125, 138-39 (2000). Warren and Brandeis have been accused of being elitist, and they were primarily concerned about intrusions into the privacy of the "upper-crust," both because they belonged to that society and because members of that society were primary targets for yellow journalists. *See id.* at 135-36.

[15] *See*, *e.g.*, Winters, *supra* note 1, at 9 (explaining how informational privacy is the ability of "individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others") (quoting WESTIN, PRIVACY AND FREEDOM, *supra* note 10). *See also* Westin, *Social and Political Dimensions*, *supra* note 10, at 431. *See generally* Gormley, *supra* note 10, at 1350.

[16] *See* Brenner, *supra* note 13, at __.

[17] *See id.* at __.

[18] *See id.* at __. *See also* Warren & Brandeis, *supra* note 10, at 198 ("[T]he legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration.").

technologies.

The need for a similar redefinition is even more pressing today, as demonstrated by the national debate over privacy interests in data maintained by health care providers, financial institutions and retail merchants.[19] Robert D. O'Harrow, Jr. has aptly captured the public's concern over data privacy:

> Law enforcement and intelligence services don't need to design their own surveillance systems . . . . They only have to reach out to the companies that already track us so well while promising better service, security, efficiency, and, perhaps most of all, convenience. It takes less and less effort each year to know what each of us is about. When we were at the coffee shop and where we went in our cars. What we wrote online, who we spoke to on the phone, the names of our friends and their friends and all the people they know. When we rode the subway, the candidates we supported, the books we read, the drugs we took, what we had for dinner, how we like our sex.
>
> More than ever before, the details about our lives are no longer our own. They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe.[20]

---

[19] *See*, *e.g.*, ERNEST F. HOLLINGS, COMM. ON COMMERCE, SCIENCE, AND TRANSP., ONLINE PERSONAL PRIVACY ACT, S. REP. NO. 107-240 (2002) (Conf. Rep.); DIV. OF FIN. PRACTICES, BUREAU OF CONSUMER PROT., U.S. FED. TRADE COMM'N, PRIVACY ON-LINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), http://www.ftc.gov/reports/privacy 2000/privacy2000.pdf.

[20] ROBERT D. O'HARROW, JR., NO PLACE TO HIDE 300 (Free Press) (2005). Mr. O'Harrow is a reporter for The Washington Post and an associate of the Center for Investigative Reporting. He was a Pulitzer Prize finalist for articles on privacy and technology and a recipient of the 2003 Carnegie Mellon Cyber Security Reporting Award. The concern is, of course, that Government could apparently obtain such information by consent even though a number of federal statutes impose restrictions on the dissemination of various types of personal data. *See*, *e.g.*, Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.512(e) (2005); Right to Financial Privacy Act, 12 U.S.C.S. § 3405 (2005); Gramm-Leach-Bliley Act 15 U.S.C.S. § 6802(e)(8) (2005); Electronic

Indeed, a recent survey of likely voters found that over 70% favored more legislation to protect the privacy of their Internet-related communications and data.[21] What created this heightened public concern? No doubt it was the creeping realization that data retention by the businesses from which we purchase the vast majority of our goods and services is not only pervasive, it is unavoidable. Such pervasive technology affects us not only when we venture into the public marketplaces, but it is intruding into our homes at an increasing rate.[22] As computer technology becomes a

---

Communications Privacy Act (ECPA), 18 U.S.C.S. § 2703 (2005). These and similar statutory provisions are not determinative of the Fourth Amendment issues discussed here because (a) the restrictions they impose are usually less than those required by the Fourth Amendment and (b) they are far more fragile than the Fourth Amendment. *See*, *e.g.*, Peter Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 916 (2004). What Congress gives, Congress can take away. Public awareness is another issue: the average American is unlikely to be aware of the provisions of these statutes (except, perhaps, to the extent that some require one to fill out paperwork), but does have at least a pragmatic grasp of Fourth Amendment guarantees.

[21] CYBER SECURITY INDUSTRY ALLIANCE, SURVEY RESEARCH ON VOTER ATTITUDES TOWARD INTERNET SECURITY ISSUES (June 15, 2005), https://www.csialliance.org/resources/pdfs/CSIA_Survey_on_Spyware_and_Identity_Theft_White_Paper.PDF.

[22] *See*, *e.g.*, "Pervasive Computing," SeachNetworking.Com Definitions, http://searchnetworking.techtarget.com/gDefinition/0,294236,sid7_gci759337,00.html [hereinafter Pervasive Computing Definition] (last visited Oct. 31, 2005).

> Pervasive computing is the trend towards increasingly ubiquitous . . . connected computing devices in the environment, a trend being brought about by a convergence of advanced electronic – and particularly, wireless – technologies and the Internet. Pervasive computing devices are not personal computers as we tend to think of them, but very tiny – even invisible – devices, either mobile or embedded in almost any type of object imaginable, including cars, tools, appliances, clothing and various consumer goods – all communicating through increasingly interconnected networks. According to Dan Russell, director of the User Sciences and Experience Group at IBM's Almaden Research Center, by 2010 computing will have become so naturalized within the environment that people will not even realize that they are using computers. Russell and other researchers expect that in the future *smart* devices all around us will maintain current information about their locations, the contexts in which they are being used, and relevant data

more and more embedded feature in every aspect of our lives, our homes are becoming equipped with technology that can be used to eavesdrop on our conversations and track our activities, even though such data collection and retention is not a primary purpose motivating its use.[23] Indeed, such technology continues to be successful in the marketplace only because its information-collection aspects are overshadowed by the benefits it provides Consumers.[24]

---

about the users.

Id.

[23] *See*, *e.g.*, Michael Kannellos, *These Walls (and Teddy Bears) Have Eyes,* CNET NEWS, June 9, 2005, http://news.com.com/These+walls+and+teddy+bears+have+eyes/2100-1040_3-5738029.html (describing presentations given at Intel Corporation's annual research day). Among the projects described were an experimental system, consisting of a series of sensors under a baby's mattress and a camera mounted on a wall, which will monitor the child's heart rate, temperature and movement; stream video of the infant; take pictures and send all the data to a parent's PC or over the Internet to a remote location. *Id*. In another experiment discussed at the conference, researchers tagged all of the items in a person's house with radio frequency identification sensors that effectively will tell a remote computer whether the occupant has moved a spoon or turned on the television. *Id*.

Dale Fuller, chief executive of Borland Software, recently described a vision of the future in which a person who had too much wine with dinner might find that his car might not start, and it might automatically call a cab, notify his spouse and even reschedule business appointments early the next morning. Ted Bridis, *Top CEOs Describe Future Technologies*, USA TODAY, June 10, 2005, *available at* http://www.usatoday.com/tech/news/2005-06-10-tech-ceos_x.htm.

[24] *See*, *e.g.*, Mahesh S. Raisinghani, et al., *Ambient Intelligence: Changing Forms of Human-Computer Interaction and Their Social Implications,* 5 J. OF DIGITAL INFO. (2004), *available at* http://jodi.ecs.soton.ac.uk/Articles/v05/i04/Raisinghani/.

> A young mother is on her way home, driving . . . with her 8-month old daughter who is sleeping in her child seat on the passenger side of the car. The infant is protected by an intelligent system called SBE 2 against airbag deployment, which could be fatal in the case of an accident. SBE 2 detects when there is a child seat on the passenger seat instead of a person and automatically disables the airbag. Arriving home, a surveillance camera recognizes the young mother, automatically disables the alarm, unlocks the front door as she

For example, efforts are underway to develop "aware homes" that incorporate intelligent, embedded systems which interact with the occupants and with outside technology.[25] An "aware home" will "be able to recognize the people that live in it, adapt . . . to them [and] learn from their behavior."[26] Similar systems will become features of offices, hotel rooms and other environments.[27] While the potential for abuses of the information-gathering capabilities of such products is particularly dramatic, the *nature and sensitivity* of the information gathered is often not inherently different from that acquired by mundane Collectors such as grocery and clothing retailers.[28]

Pervasive technology raises difficult issues about privacy, especially for those who are not users of advanced technology.[29]

> approaches it and turns on the lights to a level of brightness that the home control system has learned she likes. After dropping off her daughter, the young mother gets ready for grocery shopping. The intelligent refrigerator has studied the family's food consumption over time and knows their preferences as well as what has been consumed since the last time she went shopping. This information has been recorded by an internal tracking system and wireless communication with the intelligent kitchen cabinets. Based on this information, the refrigerator automatically composes a shopping list, retrieves quotations for the items on the list from five different supermarkets in the neighborhood through an Internet link, sends an order to the one with the lowest offer and directs the young mother there. When arriving at the supermarket, the shopping cart has already been filled with the items on her shopping list. Spontaneously, she decides to add three more items to her cart and walks to the check-out. Instead of putting the goods on a belt, the entire cart gets checked out simply by running it past an RFID transponder that detects all items in the cart at once and sends that information to the cash register for processing.

Id.

[25] *See*, *e.g.*, THE AWARE HOME, *supra* note 6; AMBIENT INTELLIGENCE, *supra* note 6. *See also* Ward, *supra* note 6.

[26] AMBIENT INTELLIGENCE, *supra* note 6. *See* Kannellos, *supra* note 23.

[27] *See*, *e.g.*, EUROPEAN COMM'N, SCENARIOS FOR AMBIENT INTELLIGENCE, *supra* note 6.

[28] *See*, *e.g.*, Rob Walker, *The Ad-Friendly World of Minority Report,* June 24, 2002, http://slate.msn.com/?id=2067293.

[29] *See*, *e.g.*, Marc Langheinrich, *Privacy by Design – Principles of Privacy-*

Most "old century" folks may think that their communications and activities are private only insofar as they shield them from observation by others. Such a view tends to associate "privacy" with enclaves such as our homes, our cars and our offices.[30] Those

---

Aware Ubiquitous Systems, *in* PROCEEDINGS OF THE THIRD INT'L CONFERENCE ON UBIQUITOUS COMPUTING 273, 273 (G.D. Abowd et al. eds. 2001), *available at* http://www.vs.inf.ethz.ch/publ/papers/privacy-principles. pdf.

> What is it that makes ubiquitous computing any different from other computer science domains with respect to privacy? . . . Four properties come to mind:
>
> Ubiquity: Ubiquitous computing is everywhere – this is its essence, its explicit goal. Consequently, decisions made in ubiquitous system and artifact design will affect large, if not every part of our lives, [sic] from crossing a street to sitting in the living room to entering an office building.
>
> Invisibility: Not only should computers be everywhere, we want them to actually disappear from our views. With the ever shrinking form factor of computing and communication devices, this goal seems far from being science fiction. Naturally, we will [sic] going to have a hard time in the future deciding at what times we are interacting with (or are under surveillance by) a computing or communication device.
>
> Sensing: As computing technology shrinks and processing power increases, so does the abilities [sic] of sensors to accurately perceive certain aspects of the environment. Simple temperature, light, or noise sensors have been around for quite some time, but next generation sensors will allow high quality audio and video feeds from cameras and microphones smaller than buttons. Even emotional aspects of our lives, such as stress, fear, or excitement, could then be sensed with high accuracy by sensors embedded in our clothings [sic] or in our environment.
>
> Memory amplification: Advancements in speech and video processing, combined with the enhanced sensory equipment available soon, make it actually feasible to perceive memory prosthesis, or amplifiers, which can continuously and unobtrusively record every action, utterance and movement of ourselves and our surroundings, feeding them into a sophisticated back-end system that uses video and speech processing to allow us browsing and searching through our past.

Id.

[30] In the *Roving Interception* case, the FBI proceeded under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351

who are accustomed to using new technology, however, are rapidly experiencing a decline in the privacy traditionally associated with these enclaves. Cell phones have basically eliminated phone booths, vehicles are equipped with surveillance technology, wireless networks and cellular communications, and information concerning much of what goes on in our homes can be obtained by third parties. Offices may be somewhat more secure, but much of our work takes place outside our offices; "road warriors" equipped with the latest in wireless communication conduct business from—and on their way to and from—other offices, and other places. The notion of "private enclaves" as places separate and apart from the world, areas in which our activities and communications are not subject to observation, is disappearing.

In this world of ubiquitous, ambient technology, "an invisible and comprehensive surveillance network" has been created, the constituent parts of which are operated by private Collectors. This network has effectively eradicated the distinction between "public" and "private" spaces.[31] Information that was historically secluded behind physical barriers now has the potential to leak into the public domain.

This emerging surveillance network has profound implications for the way law enforcement agencies approach criminal investigations. Historically, investigations involved locating the

---

(1968). Company v. United States (In re United States), 349 F.3d 1132, 1136 (9th Cir. 2003) [hereinafter *Roving Interception*]. Since Title III applies only when one has a reasonable expectation of privacy in the communications at issue, the FBI either (i) operated on the assumption that the interior of the vehicle was a "private" enclave requiring a warrant to access or (ii) proceeded under Title III because the agents needed the cooperation of the Company to exploit the System for eavesdropping purposes. *Id*. at 1136, 1145.

[31] *See* Kannellos, *supra* note 23. *See also* O'HARROW, *supra* note 20, at 291.

> Before long, our phones, laptop computers, PalmPilots, watches, pagers, and much more will play parts in the most efficient surveillance network ever made. Forget dropping a coin into a parking meter or using a pay phone discreetly on the street. Those days are slipping by. The most simple, anonymous transactions are now becoming datapoints on the vast and growing matrix of each of our lives.

presumptive situs of physical "evidence"[32] and then taking affirmative steps to find and seize that evidence.[33] The scenario had two notable characteristics. First, officers would traditionally seek evidence of a specific crime which they believed had been committed by a specific person; this focus circumscribed the scope of their efforts.[34] Second, officers would attempt to seek out and collect evidence from places associated with the suspect (because physical evidence necessarily resides in a "place").[35] Fourth Amendment analysis has consequently focused on the interaction between the officers and the suspect; the concern has been with controlling the process by which officers intrude into that person's private spaces.[36] The procedures devised to prevent "unwarranted" intrusions into personal, private spaces including strict criteria for obtaining search warrants supported by probable cause or an exception and rules narrowing the scope of authorized searches (i.e., the "plain view" doctrine), all reflect this.[37] Evidence-

---

Id.

[32] The "evidence" consists of items of tangible or intangible personal property. This includes bodily substances. *See*, *e.g.*, Schmerber v. California, 384 U.S. 757, 765 (1966).

[33] *See* Brenner*, supra* note 13, at notes __ & accompanying text.

[34] *See*, *e.g.*, WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1(a) (4th ed. 2005).

[35] Law enforcement may also seek evidence from those associated with suspects, as well as from suspects; indeed, officers may seek evidence from "civilians," i.e., those who have no involvement in the suspected criminal activity. That does not alter the structure of the dynamic outlined above. In all of these scenarios—law enforcement searches suspect's premises, law enforcement searches premises belonging to suspect's associate and law enforcement searches "civilian" premises—the inquiry is whether law enforcement violated the privacy of the person or persons whose premises were the object of a search. The focus is on law enforcement officers' actively targeting someone's premises (*Boyd*) or activity (*Katz*) for scrutiny. *See supra* Part II(A). If the officers violate someone's privacy, they can move to suppress the evidence, if any, resulting from the violation or bring a civil rights suit seeking damages for the violation. *See*, *e.g.*, FED. R. CRIM. P. 41(h); Groh v. Ramirez, 540 U.S. 551, 554-56 (2004).

[36] *See* Brenner*, supra* note 13, at notes __ & accompanying text.

[37] *See*, *e.g.*, FED. R. CRIM. P. 41(c)-(d), (e); LAFAVE, *supra* note 34, § 2.2(a). This assumption is also embedded in Title III, the legislative product of

gathering that does not intrude into such space is outside the Fourth Amendment, at least as far as the object of the search is concerned.[38]

Now, consider how this dynamic changes in a world of ubiquitous technology. In many ways, surveillance and investigation have merged. The data gathered by a surveillance network of the type outlined above,[39] along with the data Consumers generate through online or wireless communication activities, provide tremendous opportunities for law enforcement to "round up the usual suspects" even before a specific crime is reported.[40] Instead of having to search for discrete bits of

---

Katz. Title III's wiretap provisions specify that the transmission of the contents of communications is not to be interrupted by "interception;" this is simply an application of the *Jackson* principle. *See* 18 U.S.C. §§ 2510 – 2522 (2005). *See also infra* Part II.A. Instead of using an adhesive envelope, one relies upon communication systems that, it has heretofore been reasonable to assume, are "closed" to the general public. *See*, *e.g.*, U.S. Department of Justice – Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations § IV(A) (2002), http://www.cybercrime.gov/s&smanual2002.htm#_IVA_.

> Since its enactment in 1968 . . . Title III has provided the statutory framework that governs real-time electronic surveillance of the contents of communications. When agents want to wiretap a suspect's phone, "keystroke" a hacker breaking into a computer system, or accept the fruits of wiretapping by a private citizen who has discovered evidence of a crime, the agents first must consider the implications of Title III.
>
> The structure of Title III is surprisingly simple. The statute's drafters assumed that every private communication could be modeled as a two-way connection between two participating parties, such as a telephone call between A and B. At a fundamental level, the statute prohibits a third party (such as the government) who is not a participating party to the communication from intercepting private communications between the parties using an "electronic, mechanical, or other device," unless one of several statutory exceptions applies.

Id. See 18 U.S.C. § 2511(1) (2005).

[38] *See* Brenner, *supra* note 13, at notes __ & accompanying text.

[39] *See supra* notes 30–32 & accompanying text.

[40] The data gathered by these sources can be divided into three broad categories:

(i) Tool Data

Tool data encompasses personal information that is valued not for its content but for its utility. It includes Social Security numbers, dates of birth, driver's license numbers and other data; it will no doubt come to include biometric identifiers such as DNA. Tool data is a given; it is not the product of my will or effort but is assigned, more or less arbitrarily, to me. Tool data has "value" because it is an implement that can be used for good or evil: My Social Security number, for example, is a tool I can use to identify myself for various benign purposes (positive value) and one a criminal can use to steal my identity (negative value). *See*, *e.g*., Bowen v. Roy, 476 U.S. 693, 710-11 (1986).

Though tool data is something I "receive," it is not inherently "public." My Social Security number and date of birth may be "public," in that I have shared them with others, but that is not inevitable; like the other types of tool data in current circulation, they are "public" because we have not conceptualized tool data as a commodity that has "value" and must therefore be protected. The need for, and use of, tool data is a historical accident, an *ad hoc* solution to the complexity of modern society; we use tool data to identify ("I am Susan Brenner") and authenticate ("Here is proof I am Susan Brenner"). *See*, *e.g*., BRUCE SCHNEIER, BEYOND FEAR 182-95 (2003). For most of human history, these functions were relational; people were born, raised and lived their lives in the same community, where everyone knew and recognized them. *See generally id.* at 184. As populations became increasingly mobile and urbanized, relational identification and authentication no longer sufficed; it became necessary to find some surrogate, and that is what Social Security numbers, driver's licenses and other personal data became. *See*, *e.g*., Matt Sundeen, *License to Drive = Proof of Identity,* STATE LEGISLATURES, Apr. 2003, at 21.

(ii) Biographical Data

Biographical data derives from my activities in real- and cyber-space; it includes where I live and where I have lived, where I work and where I have worked, the car I drive, the routines I follow and the places and people I visit. Biographical data is considered "public" because it is the product of my behavior in "public" places, where what I do can be observed by anyone who shares that space with me. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003). Consequently, biographical data, defined as information which was or could have been obtained by observing activity in a "public" place, is not private under *Katz* or under cognate tests used to implement civil privacy protections. *See* United States v. Knotts, 460 U.S. 276, 282-85 (1983); *Remsburg*, 816 A.2d at 1009. As Part II explained, the implementation of ubiquitous technology makes the assumptions underlying this category increasingly problematic because it is based on a purely spatial bifurcation of "public" and "private."

(iii) Transactional Data

Transactional data is generated by our interactions with others. In analyzing the privacy of transactional data, it is useful to divide it into two types: (a) professional transactional data, which results from interactions with attorneys, physicians, religious advisors, psychiatrists, accountants and other professionals; and (b) commercial transactional data, which results from interactions with those who provide commercial goods or services offline or online. There are certain constants across these categories: Each generates data which establishes (i) that I interacted with a particular professional or commercial resource on one or more occasions, (ii) the nature of that interaction (seeking legal advice, making a purchase) and (iii) the details of that interaction (seeking legal advice about an estate, purchasing vitamins or electronics or clothing). None of this data is private under the *Katz* test or cognate civil standards because by interacting with external entities (human or automated) I have knowingly exposed (i)-(iii) to public view; I assumed the risk that those with whom I interact will reveal the details of that interaction to others.

There can be some overlap between transactional data and biographical data. To understand why, it is useful to consider two real-world transactions: In the first, I consult with an attorney whose office is in my neighborhood; in the second, I purchase a prescription from a pharmacist at my local drug store. My traveling to the law office and to the drug store takes place in "public," and so can be considered biographical data. It is also transactional data insofar as it shows that I interacted with the lawyer and with the pharmacist. These respective encounters differ somewhat in the extent to which the nature and details of the interactions are biographical. My purchasing a prescription from the pharmacist takes place in "public," and so the nature of the transaction tends toward the biographical; but the details of the purchase will remain confidential unless I choose to share them or unless the pharmacist is indiscreet enough to announce the nature and uses of the medication I buy. Since it is reasonable to infer that I went to a law office to obtain legal advice, the nature of that transaction also tends towards the biographical; but since the transaction itself does not take place in "public," the details do not constitute biographical data.

The law has treated the categories differently: Professional interactions are usually encompassed by privileges that bar the professional from revealing details of the interaction without the client's permission; the purpose is to provide confidentiality when it is "essential to the full and satisfactory maintenance of the relationship between the parties." PAUL F. ROTHSTEIN & SUSAN W. CRUMP, FEDERAL TESTIMONIAL PRIVILEGES § 1.1 (2d ed. 2004). For commercial interactions, the general rule is that "the facts of a transaction belong jointly and severally to the participants. If Alice buys a chattel from Bob, ordinarily both Alice and Bob are free to disclose this fact." A. Michael

information from a disjointed array of physical sources, officers can "harvest" information held by these private Collectors.[41] The harvest can occur either as a result of Government's purchase of

---

Froomkin, *The Death of Privacy?,* 52 STAN. L. REV. 1461, 1521-22 (2000) (noting that a "very small number of statutes impose limits upon the sharing of private transactional data collected by persons not classed as professionals"). Neither type of transactional data is private in the constitutional-common law sense, but the evidentiary and other constraints American law places on the dissemination of data resulting from professional interactions limit its circulation to those involved in the professional consultation; therefore, while professional transactional data is not private, it is secured.

[41] *See*, *e.g.*, Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment,* 8 VA. J.L. & TECH. 6, ¶¶ 2-3 (2003).

> The Internet was initiated by the State, and soon after was privatized . . . . Market powers . . . facilitated the rise of new players . . . who gained power and control in the information environment . . . . A convergence of interests seems to be developing among players such as copyright owners and service providers on the one hand, and the State's growing interest in the digital environment, on the other hand. Law enforcement agencies seek to enhance their monitoring capacity and online businesses seek to prevent fraud and combat piracy while strengthening their ties with authorities. This convergence might lead to an unholy alliance with potentially troublesome results . . . .
>
> The most explicit example . . . is reflected in a presentation by Joseph E. Sullivan, director of compliance and law enforcement relations at eBay. Addressing law enforcement agents at a conference on cybercrime, Sullivan offered to hand over information, when requested . . . . eBay is one of the largest online e-commerce businesses, and the owner of PayPal, which provides clearing services for online financial transactions. eBay controls access to a colossal amount of information, including financial records, names, user IDs and passwords, affiliations, e-mail addresses, physical addresses, shipping information, contact information, and transaction information (i.e., bidding history, prices paid, feedback rating). But eBay is not alone in implementing law enforcement-friendly policy. The emerging regime of recent years facilitates cooperation between the State and the private sector in law enforcement efforts, beyond the reach of judicial review.

Id.

data or from a "request." Either way, the Government's ability to obtain and sift huge amounts of Consumer data without any reason to believe a crime has been committed dwarfs anything that could have been accomplished by the general warrant procedure that led to adoption of the Fourth Amendment.[42]

A fairly recent Ninth Circuit case illustrates how far we have come. *In re U.S. for an Order Authorizing Roving Interception of*

---

[42] Brenner, *supra* note 13, at __. *See* Florence Olsen, *Lawmakers Have Tough Questions for Largely Unregulated Data Firms,* Federal Computer Week (Apr. 25, 2005), http://www.fcw.com/ article88676**.**

> FBI officials spent $75 million last year for information from data aggregators, a fast-growing and largely unregulated market . . . .
>
> The FBI buys information from data aggregators ChoicePoint, credit bureau reporting companies, Dun and Bradstreet, LexisNexis, the National Insurance Crime Bureau and Westlaw, which agents use mainly for convenience, said Chris Swecker, assistant director of the FBI's Criminal Investigative Division.
>
> "Twenty-three years ago when I first came to the FBI, I had to walk down to the courthouse to get courthouse records and go other places to collect these records," Swecker said. "Being able to make one query and get all these records at one time saves investigative time and saves resources," he said.
>
> Records that the FBI finds useful include driver's license information, last known address, date of birth, court filings, liens and newspaper records, Swecker said, adding that FBI officials conducted 1.2 million queries in the ChoicePoint database in 2004.
>
> Privacy experts say federal agencies' use of commercial databases creates a problem. "It allows them . . . to outsource data-collection activities," said James Dempsey, executive director of the . . . Center for Democracy and Technology. If federal officials start a new collection of data, they must comply with the Privacy Act, which requires agencies to perform a privacy impact assessment, Dempsey told the committee. But when government officials buy that data or subscribe to data that they don't pull into a government database, none of the Privacy Act rules apply, Dempsey said . . . .
>
> Sen. Russell Feingold . . . said he is concerned there are no guidelines to ensure that information in commercial databases is used responsibly. Without restrictions, there is nothing to prevent federal agencies from using commercial data "for privacy-intrusive data-mining programs," he said.

Id.

Oral Communications[43] arose from the Federal Bureau of Investigation's efforts to use technology integrated into a private vehicle to intercept conversations taking place within it.[44] As the Ninth Circuit explained, some vehicles are equipped with "telecommunication devices" that assist with navigation or with "emergencies or obtaining road-side assistance. Such systems operate via a combination of GPS . . . and cellular technology."[45] The appellant in the case (the Company) operated one such service (the System).[46] One feature of the System let the Company open a cellular connection to a vehicle and listen to conversations in the car.[47] The purpose was to help recover stolen vehicles, but it could also be used to eavesdrop on legitimate conversations conducted in a vehicle equipped with the System.[48] Realizing this, the FBI obtained "orders requiring the Company to assist in intercepting conversations taking place in a car equipped with the System."[49]

The FBI in effect "harvested" the conversations held in the target vehicle. This case highlights issues we will face as technology becomes an increasingly pervasive feature of our lives.[50] We have for many decades assumed that a vehicle is a private place; fictional characters often take advantage of the privacy a vehicle offers to discuss sensitive matters.[51] The privacy

---

[43] 349 F.3d 1132 (9th Cir. 2003).

[44] Law enforcement installation of listening devices in vehicles is far from novel. *See*, *e.g*., Massiah v. United States, 377 U.S. 201 (1964) (detailing how in 1959, federal agents installed a "Schmidt radio transmitter" under the front seat of a car and used it to listen in on conversations held by the occupants of the vehicle).

[45] *Roving Interception*, 349 F.3d at 1133.

[46] *Id.*

[47] *Id.*

[48] *Id.* at 1133-34.

[49] *Id.* at 1134.

[50] *See*, *e.g*., Centre for Pervasive Computing, http://www.pervasive.dk/.

[51] In the *Roving Interception* case, the court focused exclusively on a specific statutory structure created for the authorization and implementation of wiretaps, so the question of whether the interior of the vehicle was a "private" place was not raised, though it was presumably assumed. *Roving Interception*, 349 F.3d at 1133.

of vehicles has, of course, been compromised on occasion;[52] while we might be aware, at some level, that cars could be "bugged," we could not imagine that our vehicles would themselves become instruments of surveillance.

If cars can become instruments of surveillance, what about our homes? The case discussed above illustrates a trend—the pervasiveness of technology—that will surely find its way into our homes.[53] As computer technology increasingly becomes entrenched in every phase of our lives, our homes, too, will come equipped with technology that can be used to eavesdrop on our conversations and track our activities; interactive electronic devices will be embedded in appliances, clothing, furniture and the home itself.[54] Interacting with these embedded technologies will become a necessary and inevitable aspect of our lives; our home will regulate the internal environment, order groceries and arrange for other essential services without being asked to do so.[55] While these technologies will make our lives easier, they will also

---

[52] *See supra* note 43-49 & accompanying text.

[53] *See*, *e.g.*, Pervasive Computing Definition, *supra* note 22.

[54] *See* Kannellos, *supra* note 23 & accompanying text. *See also* Marc Langheinrich et al., *Living in a Smart Environment: Implications for the Coming Ubiquitous Information Society,* 15 TELECOMMUNICATIONS REV. 5 (Feb. 2005), *available at* http://www.vs.inf.ethz.ch/publ/papers/sktelecom 2005.pdf.

> By virtue of its very definitions, the vision of ubiquitous computing has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life: "The old sayings that 'the walls have ears' and 'if these walls could talk' have become the disturbing reality. The world is filled with all-knowing, all-reporting things." . . . Today's economic reality – shopping without participating in comprehensive profiling [–] . . . might become an expensive luxury for well-off citizens.

(quoting R. Lucky, *Everything Will Be Connected To Everything Else*, IEEE SPECTRUM (Mar. 1999), http://www.argreenhouse.com/papers/rlucky/ spectrum/ connect.shtml).

[55] *See*, *e.g.*, Kelly Greene, *Take A Glimpse Inside the Home of the Future*, REAL ESTATE JOURNAL (May 24, 2004), http://www. realestatejournal.com/housegarden/indoorliving/20040524-greene.html. *See also* Mark Weiser, *Open House* (Mar 1996), http://www.dcs.gla.ac.uk/ ~matthew/lectures/HCI4/ weiserOpenhouse.pdf.

"broadcast" personal information to a variety of external sources.

Like the System, this technology will be included because it has other valuable uses.[56] And like the System, much of this technology will operate below our personal radar; that is, like the driver and passengers upon whom the FBI eavesdropped, we will remain unaware that embedded technology is tracking and preserving the details of our actions, our conversations and even our vital signs.

With pervasive technology, the focus on privacy shifts from intrusions into spaces under the Consumer's temporary or permanent control, to the acquisition of information from sources over which the Consumer has contractual rights but no effective *ex ante* control or even a right of access to the database containing the stored information.[57] This "harvesting" scenario represents a twenty-first century variation of the "assault on the castle" scenario

---

[56] *See*, *e.g.*, Raisinghani, *supra* note 24.

[57] We do not mean to suggest that this information "harvesting" scenario will supplant the traditional dynamic of Government intrusions into privacy. We are physical beings and, as such, will continue to act, and to generate physical evidence, in the real-world; the primary locus of evidence for traditional crimes such as rape, murder and drug trafficking will no doubt remain in the real-world. But even those crimes may involve stored transactional data. *See*, *e.g.*, Eric Weslander, *Web Evidence Used in Murder Hearing,* LAWRENCE JOURNAL-WORLD (Kansas), Dec. 10, 2004, *available at* http://www.ljworld.com/section/crime_fire/story/189998.

> The case of a Kansas State University professor charged with murdering his ex-wife headed into uncharted legal territory Thursday as prosecutors presented evidence of an Internet search history from the suspect's computers . . . .
>
> A Lawrence Police detective who examined computers seized from Thomas E. Murray testified that in the month before Carmin D. Ross' killing, Murray's computers had been used to search the Internet for phrases that included "how to hire an assassin," "how to kill someone quickly and quietly" and "how to murder someone and not get caught."

Id. The detective "testified that even though Murray appeared to use his computer regularly on Thursday mornings, there was virtually no file activity on Murray's computers the morning of Nov. 13, 2003, the day prosecutors allege he drove to Lawrence and stabbed and beat Ross to death." *Id*.

that ultimately prompted the adoption of the Fourth Amendment.[58]

To understand this scenario, and its relationship to the "harvesting" scenario, we need to briefly review the history of the Fourth Amendment. The Fourth Amendment is intended to protect the sanctity of private property from intrusions by public officials;[59] its concern with protecting private property derives from common law.

Early English common law punished "those who invaded a neighbor's premises."[60] By the twelfth century housebreaking was one "of the more serious crimes in medieval England," and by the sixteenth century English law had developed specific prohibitions against housebreaking, burglary and trespass.[61] These laws were concerned only with trespasses by private persons because official searches of private premises were almost unknown until the fifteenth century.[62] In the latter half of the fifteenth century, the King and Parliament began authorizing trade guilds to "enter and search the workmanship of all manner of persons" to enforce guild regulations.[63] Roughly a century later, the Court of the Star Chamber, charged with licensing books and regulating printing

> [D]ecreed that the wardens of the Stationers' Company . . . should have authority to open all packs and trunks of papers and books brought into the country, to search in any warehouse, shop, or any other place where they suspected a violation of the laws of printing to be taking place [and] to

---

[58] *See*, *e.g.*, Wilson v. Layne, 526 U.S. 603, 609-10 (1999).

[59] *See*, *e.g.*, Boyd v. United States, 116 U.S. 616, 627 (1886).

[60] *See*, *e.g.*, William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning 32 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with author).

[61] *Id.* at 31-35.

[62] *Id.* at 36, 75. A law enacted in 1335 required innkeepers in ports to search guests for counterfeit money; the innkeepers kept a portion of whatever they found and turned the rest over to "official searchers" who took the rest and monitored the innkeepers' discharge of this obligation. *See* LASSON, *supra* note 5, at 23.

[63] *See* LASSON, *supra* note 5, at 24.

seize the books printed contrary to law."[64]

Other courts followed suit, issuing edicts authorizing similar searches directed at those suspected of libel, heresy and political dissent.[65] This led to the evolution of the general warrant, which these courts issued with no proof of individualized suspicion and in which no "names are specified . . . and . . . a discretionary power was given to messengers to search wherever their suspicions may chance to fall."[66] As arbitrary searches became more common, "Englishmen began to insist that their houses were castles for the paradoxical reason that the castle-like security that those houses had afforded from intrusion was vanishing."[67]

In the eighteenth century, English courts responded to citizens' concern about "assaults on their castles" by issuing a series of decisions that held that homes were protected from arbitrary action by government officials.[68] Most of these decisions grew out of one infamous investigation of seditious libel. Ordered to find the author of a recently-published letter, officers acting under the authority of a general warrant searched five houses and made a number of arrests.[69] Those whose homes were searched sued the officers who conducted the searches for trespass, and the government "undertook the responsibility of defending all actions arising from the warrant and the payment of all judgments."[70] To the delight of

---

[64] *Id.* at 25. The Stationers' Company was a guild of printers charged with enforcing the Star Chamber's restrictions on printing. *See*, *e.g.*, TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 25 (1969).

[65] *See* LASSON, *supra* note 5, at 25-27. "No limitations seem to have been observed in giving messengers powers of search . . . in ferreting out . . . evidence. Persons and places were not necessarily specified, seizure of papers and effects was indiscriminate, everything was left to the discretion of the bearer of the warrant." *Id.* at 26. *See also* Cuddihy, *supra* note 60, at 100-19.

[66] LASSON, *supra* note 5, at 45 (quoting Wilkes v. Wood, 98 Eng. Rep. 489 (C.P. 1763)).

[67] Cuddihy, *supra* note 60, at 128. *See* LASSON, *supra* note 5, at 30-45.

[68] *See* Money v. Leach, 97 Eng. Rep. 1050 (K.B. 1765); Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765); *Wilkes*, 98 Eng. Rep. 489; Huckle v. Money, 95 Eng. Rep. 768 (C.P. 1763).

[69] *See* LASSON, *supra* note 5, at 43-45.

[70] *Id.* at 45.

the British public, the plaintiffs won, and their verdicts were upheld on appeal.[71] Encouraged by their success, John Entick, the victim of a similar search, sued the officers who searched his home for trespass and won a verdict of £300.[72] The Court of Common Pleas upheld the verdict:

> Our law holds the property of every man so sacred that no man can set his foot upon his neighbour's close without his leave; if he does, he is a trespasser . . . . The defendants have no right to avail themselves of . . . these warrants . . . . [W]e can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society.[73]

The effect of the *Entick* opinion and other decisions was to apply the same standard to public and private actors: In either instance, a trespasser could be held civilly liable for entering another's property "without a lawful authority."[74]

The English notion that "a man's house was his castle" came to America with the colonists.[75] "Between 1754 and 1788, Americans often resorted to house-as-castle rhetoric in condemning excise taxes, general warrants and writs of assistance, a type of those warrants that was used to collect import duties."[76] The colonists were particularly outraged by the writs of assistance, and waged an unsuccessful legal battle against them during this period.[77] The resentment these writs generated was a driving factor in the Revolution and, later, in the adoption of bills of rights by states and

---

[71] *See id.* at 44-46.

[72] *See id.* at 47. *See also Entick*, 95 Eng. Rep. at 807-08.

[73] *Entick*, 95 Eng. Rep. at 817.

[74] WILLIAM BLACKSTONE, III COMMENTARIES ON ENGLISH LAW 163, (William Morrison, ed., 2001).

[75] *See* Cuddihy, *supra* note 60, at xcvi ("[T]he familiar quotation appeared in the colonies no later than 1647, in Rhode Island's first code of laws.").

[76] *Id.* at xcvii.

[77] *See*, *e.g.*, LASSON, *supra* note 5, 51-61. "[A]ny person who was authorized by a writ of assistance" was permitted to "search any house, shop, warehouse, etc.; break open doors, chests, packages, . . . and remove any prohibited or uncustomed goods or merchandise." *Id*. at 53.

by the federal government.[78] The Fourth Amendment was therefore a product of the same concerns that resulted in the law of trespass being applied to public actors: "to guard individuals against improper intrusion into their buildings where they had the exclusive right of possession."[79] It was intended to secure spatial privacy—to restrict law enforcement's ability to break down doors and rummage through rooms, boxes, chests and drawers.

II. THE FOURTH AMENDMENT, THIRD PARTY RECORDS AND TECHNOLOGICAL ADVANCES

We now turn to the Supreme Court's approach to the privacy of third party records, which arose in situations far different from that presented by current electronic database technology. The sections below address that approach in two steps. Section A describes how the Supreme Court has interpreted the Fourth Amendment's applicability to searches and seizures of transactional records held by third parties in light of twentieth century technological advances.[80] Section B explains why that

---

[78] *See id.* at 51-61, 79-82. *See also* Marshall v. Barlow's, Inc., 436 U.S. 307, 310-11 (1978) ("[The] Fourth Amendment's commands grew in large measure out of the colonists' experience with the writs of assistance . . . [that] granted sweeping power to customs officials and other agents of the King to search at large for smuggled goods.") (internal citation and quotation omitted).

[79] Jones v. Gibson, 1 N.H. 266, 272 (1818).

[80] The discussion of Supreme Court cases in this section is selective: It is limited to cases that have dealt with the use of new communicative technologies, as defined in note 1, *supra*. The Court has used the *Katz* standard to decide whether a wide variety of police conduct constitutes a "search" under the Fourth Amendment. *See*, *e.g.*, Florida v. Riley, 488 U.S. 445, 450-51 (1989) (holding that it is not a search for police to fly over a greenhouse in a helicopter and observe marijuana plants through gaps in its roof); California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (holding that it is not a search for police to fly over a backyard in commercial airspace and view marijuana being grown there); Dow Chemical v. United States, 476 U.S. 227, 239 (1986) (holding that it is not a search to fly over a chemical plant and photograph the premises). The "technologies" at issue in these cases were simply tools police used to gain a favorable physical vantage point from which to make observations with the unaided, or aided, naked eye; these cases did not involve the type of pervasive,

approach is inadequate to protect the societal interest in maintaining the privacy of digital transactional data.

A. Third Party Records and Twentieth Century Technology

The Supreme Court has addressed the application of the Fourth Amendment to communicative technologies only a handful of times in the last fifty years. Even more disappointing is that the Court has addressed these issues in an inconsistent and unprincipled manner.[81] The foundational case is *Katz v. United States*,[82] a 1967 case in which the Court held that warrantless Government wiretapping violated the Fourth Amendment, thereby overruling its 1928 decision in *Olmstead v. United States*.[83]

Katz was convicted of violating 18 U.S. Code § 1084, which makes it a crime to use facilities of interstate commerce to transmit wagering information.[84] The conviction was based on six tape recordings which were obtained by means of an electronic listening device attached to the outside of the public telephone booth.[85] The authorities conducted the eavesdropping after discovering that Katz used these phones to call a know gambler. Notwithstanding this information, the authorities made no effort to obtain judicial authorization for the eavesdropping.[86]

Katz raised two issues in his appeal, both of which involved the relationship between the Fourth Amendment and a "constitutionally protected area."[87] The Court declined to accept

---

autonomous technologies analyzed in this article.

[81] For an extensive examination of the Court's decisions addressing privacy interests as affected by advances in communicative technologies, see Brenner, *supra* note 13, at __.

[82] 389 U.S. 347 (1967).

[83] 277 U.S. 438 (1928).

[84] *Katz*, 389 U.S. at 348-49.

[85] *Id*. at 354 n.14.

[86] *Electronic Surveillance*, 82 HARV. L. REV. 187, 187-88 (1968).

[87] *Katz*, 389 U.S. at 349-51. To this point in history, Fourth Amendment violations occurred only when there was a physical trespass onto a "constitutionally protected area." *See*, *e.g.*, Erik G. Luna, *Sovereignty and Suspicion*, 48 DUKE L.J. 787, 793 n.20 (1999). In an attempt to come within that

his formulation, explaining that the resolution of "Fourth Amendment problems is not . . . promoted by incantation of the phrase 'constitutionally protected area.'"[88] The majority went on to announce a new Fourth Amendment standard:

> [T]he parties have attached great significance to the . . . telephone booth from which the petitioner placed his calls. The petitioner has . . . argued that the booth was a "constitutionally protected area." The government has maintained . . . that it was not. But this effort . . . deflects attention from the problem presented by this case. *For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*.[89]

In an important concurrence, Justice Harlan articulated the standard that has been used in later decisions to implement the *Katz* holding:[90]

> As the Court's opinion states, "the Fourth Amendment protects people, not places." The question . . . is what protection it affords to those people . . . . *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,*

---

doctrine, Katz argued that when he

> occupied [the phone booth] for the purpose of engaging in a personal conversation and closed the door to the booth, he [was] in effect in his own residence. By invitation from the telephone company and the payment of the toll he says he is entitled to consider the booth protected from intrusion by the Fourth Amendment.

Katz v. United States, 369 F.2d 130, 133 (9th Cir. 1966), *reversed by* 389 U.S. 347 (1967).

[88] *Katz*, 389 U.S. at 348.

[89] *Id.* at 351 (citations omitted, emphasis added).

[90] The Court adopted Harlan's "reasonable expectation of privacy" standard in Terry v. Ohio, 392 U.S. 1, 9 (1968), and has applied it ever since.

> *second, that the expectation be one that society is prepared to recognize as "reasonable."* Thus a man's home is, for most purposes, a place where he expects privacy . . . . On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[91]

Katz, of course, involved the interception of the contents of communications between two individuals, not government seizures of records held by third parties. But since the *Katz* Court characterized its holding as the general standard that would be used to determine whether a Fourth Amendment right to privacy existed, *Katz* shaped how the Court approaches third-party records, as well as real-time personal communications.

In the next dozen years, the Supreme Court twice considered whether the Fourth Amendment applies when Government obtains records pertaining to an individual that are generated and held by a party with whom the individual has commercial dealings. In the parlance of this article, the question was whether Government could obtain without a warrant Data generated and maintained by a Collector reflecting transactions between the Collector and the Consumer/defendant. In *United States v. Miller*,[92] Miller, who had been indicted on tax charges, moved to suppress records concerning his bank account; federal agents had obtained the records by using a grand jury subpoena, not a warrant.[93] The Court

---

[91] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (emphasis added). It is important to note that Justice Harlan interpreted the majority's opinion as holding "only" (i) that a telephone booth is an area in which one "has a constitutionally protected reasonable expectation of privacy;" (ii) that electronic invasions, as well as physical invasions, of such an area can violate the Fourth Amendment; and (iii) that the invasion of a "constitutionally protected area" without a warrant is presumptively unreasonable. *Id.* at 360-61. His standard therefore implicitly incorporates the spatially-based conception of privacy that had prevailed since *Olmstead*. Olmstead v. U.S. 277 U.S. 438, 479 (1928). This is evident in his comment that the rule he cites "emerged from prior decisions." *See supra* note 91 & accompanying text. Those decisions were, by necessity, based on *Olmstead*'s trespass doctrine.

[92] 425 U.S. 435, 436 (1976).

[93] *Id.* at 437.

of Appeals for the Fifth Circuit held that the agents had "improperly circumvented" his Fourth Amendment rights.[94] The Supreme Court in 1976 disagreed: "We find that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress."[95] This post-*Katz* Court cited a pre-*Katz* opinion for the proposition that "'no interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'"[96] *Katz*, of course, rejected the use of "constitutionally protected area" as the touchstone of Fourth Amendment privacy. The *Miller* Court also noted that "the documents subpoenaed here are not respondent's 'private papers.' . . . [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks."[97]

In *Miller*, the Court clearly misapplied its own precedent. First its focus on a "constitutionally protected area" ignored *Katz*'s statement that the Fourth Amendment protects "*people and not places*."[98] Second, by focusing on the owner of property, the Court ignored the holding of *United States v. Matlock*[99] that the protections of the Fourth Amendment do not rest upon the law of

---

[94] *Id.* at 438.

[95] *Id.* at 440.

[96] *Id.* (quoting Hoffa v. United States, 385 U.S. 293, 301-02 (1966)).

[97] *Miller*, 425 U.S. at 440. The *Miller* Court's only references to *Katz* came in the paragraph in which it addressed Miller's reliance on the *Katz* Court's statement that "we have . . . departed from the narrow view" that "'property interests control the right of the Government to search and seize.'" 425 U.S. at 442 (quoting Katz v. United States, 389 U.S. 347, 353 (1967) (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)). The *Miller* Court dismissed this aspect of *Katz*, noting that the *Katz* Court "stressed that '[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'" 425 U.S. at 442 (quoting *Katz,* 389 U.S. at 351). The *Miller* Court then proceeded to base its holding on the *Katz* "assumption of risk" principle. *Id*.

[98] *See supra* note 89 & accompanying text.

[99] 415 U.S. 164 (1974).

property, "with its attendant historical and legal refinements."[100] The question the Court should have addressed was not to whom the records belonged, but whether it is in our society's interest to condition a Consumer's use of the nation's banking system on a waiver of his Fourth Amendment privacy.

Three years later, the Court decided *Smith v. Maryland.*[101] *Smith* was the "other half" of *Katz*; the issue was "whether the installation and use of a pen register," which captures the numbers dialed on a telephone, "constitutes a 'search' within the meaning of the Fourth Amendment."[102] The *Smith* Court began its opinion by reviewing *Katz* and noting that the standard used to implement *Katz* is the two-pronged test Justice Harlan enunciated in his concurring opinion: (i) whether the individual has exhibited a subjective expectation of privacy in the thing, place or endeavor; and (ii) whether society is prepared to regard the individual's subjective expectation of privacy, if any, as reasonable.[103]

The Court found that Smith met neither criterion:

> Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner . . . cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area." Petitioner's claim . . . is that, notwithstanding the absence of a trespass, the State . . . infringed a "legitimate expectation of privacy". . . . [A] pen register differs . . . from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of

---

[100] *Id.* at 172 n.7. The issue in *Matlock* was whether one's authority to consent to a search by law enforcement derived from a property interest in the place or thing to be searched. *Id.* The case involved the validity of a consent to search given by the co-occupant of a house. *Id.* at 166. Since the co-occupant was neither the owner nor the lessor of the property, her consent to search would not have been valid if the authority to consent was a function of her having a property interest in the house. As noted above, the Supreme Court rejected this narrow interpretation of one's authority to consent to a search, to an invasion of privacy, in favor of a broader standard. *Id.* at 172.

[101] 442 U.S. 735 (1979).

[102] *Id.* at 736.

[103] *Id.* at 740. *See infra* Part II.B.3.

communications . . .

> [P]etitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone . . . .
>
> [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 telephone company switching equipment that their calls are completed. All subscribers realize . . . 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 . . . . Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[104]

The Court also rejected Smith's claim that he demonstrated a subjective expectation of privacy by making the calls from his home,[105] and held that, even if he could show such a subjective

---

[104] *Smith*, 442 U.S. at 741-43 (citations omitted).

[105] *Id.* at 743.

> [T]he site of the call is immaterial . . . . Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company . . . if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

expectation, it is not one society would regard as reasonable: "[E]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as 'reasonable.'" The Court went on to state that it has consistently held "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[106]

Smith, therefore, suffers from the same weakness as *Miller*. It applies an assumption of the risk rationale to a situation in which the Consumer actually has no choice but to forego privacy expectations unless he is willing to forego a material, if not practically essential, service.[107]

The Supreme Court has applied the *Miller-Smith* principle in a variety of cases.[108] It summarized the rationale for the principle in *United States v. Jacobsen*:

> [W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does

---

Id.

[106] *Id.* at 743-44 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)) (citing *Miller*, 425 U.S. at 442-44).

[107] *Smith* is also distinguishable on its facts from most of the situations we address. The Court based its decision in large part on the fact that subscribers had to know from their bills that the phone company kept records of numbers dialed. *Smith*, 442 U.S. at 744. The same assumption cannot be made about the extent to which Consumers understand or appreciate the nature of data collection or mining or the extent to which database technology can compile and aggregate information about disparate transactions.

[108] *See*, *e.g*., California v. Greenwood, 486 U.S. 35, 41-42 (1988) (applying *Smith*'s assumption of risk analysis to hold it was not a search for police to fly over individual's back yard to discover marijuana plants); S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 735-36, 743 (1984) (holding that *Miller* foreclosed "respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers").

> not prohibit governmental use of the now non-private information . . . . The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.[109]

The *Jacobsen* Court therefore construed privacy as an ephemeral concept—as something that vanishes absolutely once access to information has been shared with others. In short, the Court has applied an assumption of risk analysis that makes informational privacy a purely zero-sum (i.e., private or not-private) concept. A Consumer who fails to keep information solely to herself loses all Fourth Amendment protection. This is, as we explained above, applying an eighteenth-century bricks-and-mortar conception of privacy to a world that has been, and is being, fundamentally altered by rapidly-evolving, pervasive technologies.[110]

B. The Inadequacy of Twentieth Century Analysis for Twenty-First Century Technology

Miller and *Smith* evince an unarticulated assumption that the Fourth Amendment conception of privacy is zero-sum. If that were true, then Consumers have no control over the information they (knowingly, unknowingly, willingly or unwillingly) provide to others regardless of the extent to which that information is personal or private and whether it is required for the purchase of goods or services that are necessary or even desirable for meaningful participation in twenty-first century society. In other words, as computer technology becomes more embedded in society, consumers will be increasingly forced to waive their Fourth

---

[109] 466 U.S. 109, 117 (1984) (emphasis added). The issue in *Jacobsen* was the propriety of law enforcement agents' observing evidence that had been brought to their attention by private parties. *Id.* at 111. The Court held, essentially, that since the private parties' observation of the evidence had already compromised Jacobsen's privacy interest in it, the subsequent viewing by law enforcement did not constitute a "search" under the Fourth Amendment. *Id.* at 118-19.

[110] *See supra* notes 1-5 & accompanying text.

Amendment rights in order to obtain vital goods and services. We must consider, therefore, whether the Supreme Court's approach is justified.

With all due respect to the Court, we submit that its zero-sum construct reflects at least five errors. First, it ignores the sound two-pronged approach of *Katz*. Second, it wrongly assumes that the mere transmittal of data constitutes a *disclosure* of information. Third, it erroneously concludes that a disclosure to a person who has promised to maintain the confidentiality of that information is a disclosure to the *public*.[111] Fourth, it would apply the assumption of risk construct even when (a) the Consumer enters into a transaction by which she does not accept that risk and (b) the disclosure is an inherent component of a socially beneficial or necessary relationship such that she would have to forego that relationship to avoid the disclosure.[112] Fifth, holding that the consent of a Collector to a Government request for information overcomes the Consumer's privacy interest reflects an inappropriate balancing of society's interest in privacy versus Government's interest in investigation. The sections below outline our analysis of each of these issues.

---

[111] The Court did not focus in *Miller* or *Smith* on the contractual interests of the Consumer or the Collector. The analysis appears to have been more akin to a tort concept of assumption of the risk. We note that the fact that a Consumer might have a claim for breach of contract against the Collector who discloses private Data should not affect the issues addressed here if only because (i) any contractual remedy would come too late to protect the Consumer's privacy interest and (ii) it would be extremely difficult to translate the harm to the Consumer into monetary damages.

[112] Thus, disclosures to third parties such as Internet Service Providers, health insurers and smart home services vendors differ fundamentally from the types of disclosures that Warren and Brandeis addressed. The Warren-Brandeis article was concerned with disclosures made that were made to other people by chance, i.e., by being in a particular place at a particular time. One could argue that the element of choice is missing, but there is another difficulty with assuming privacy in this context: The complained-of information (photography, description of what someone did) was gathered in an ostentatiously public place—a street, a restaurant, a hotel, etc. It is, after all, inevitable that certain of our actions will occur in public spaces; we cannot insist that our every action is private and must be ignored.

1. Application of the Katz *Two-Part Test Supports Fourth Amendment Protection to Collector-Stored Data*

As noted above,[113] the Supreme Court in *Smith* accepted Justice Harlan's formulation of the *Katz* holding as the standard governing Fourth Amendment privacy analysis: "My understanding of the rule . . . 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.'"[114]

---

[113] *See supra* note 111 & accompanying text.

[114] *Katz*, 389 U.S. at 361. The Court in *Smith* calls *Katz* the "lodestar" for determining the application of the Fourth Amendment and specifically recognized the accuracy of the Harlan restatement:

> This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy,"—whether, in the words of the *Katz* majority, the individual has shown that "he seeks to preserve [something] as private." The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'"—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances.

Smith, 442 U.S. at 740-41 (citations and note omitted). Note that Justice Blackmun in *Smith* inserts the term "viewed objectively" in stating the *Katz* holding, whereas *Katz* used no such term but instead appears to be referring to "justifiable" in the sense of consistent with societal interests. Thus, *Katz*'s holding is stated as follows:

> The government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.

Katz, 389 U.S. at 352. Immediately following, the Court explained its rationale:

> One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Miller and *Smith*, however, ignore that formulation in favor of a single-pronged assumption of risk test. In so doing, they ignore fundamental safeguards intrinsic in the two-part test. The "subjective" element has historical roots that predate even the Constitution.[115] Those roots demonstrate that the only justifiable substantive qualification of the subjective element is that it is evaluated in light of all facts and circumstances known to the Consumer.[116] The reason for this should be obvious. Although the purpose of the Fourth Amendment is to promote reasonable Government action, even reasonable Government action is subordinate to society's interest in honoring generally accepted expectations as to what is, and what is not, private.

Miller and *Smith* depart from that subjective standard by applying an objective test based on what judges think reasonably knowledgeable citizens know. Thus, in holding that a bank customer assumes the risk of providing information to his bank, the Court is really saying that the customer's expectation that his records will remain private is categorically unreasonable. That is not a valid assessment of the customer's subjective assessment of risk, however, but an objective evaluation.

Nor can the *Miller-Smith* assumption of risk test be justified on the basis of the second, objective prong of the *Katz* formula. The *Miller-Smith* test considers only the empirical question of whether the Consumer should have held her subjective belief—that is, whether she should have expected potential additional disclosures to third parties.[117] The second *Katz* prong, however, makes

---

Id. This explanation demonstrates that it is not just the precautions the caller takes to protect his privacy by closing the door that entitles him to rely on the Fourth Amendment, it is also the fact that telephone communication plays a vital role in society and therefore is worthy of protection.

[115] *See*, *e.g.*, SMITH, *supra* note 14, at 8-47 (describing conceptions of privacy in American colonies).

[116] *See* Brenner, *supra* note 13, at __.

[117] *Miller* recognized that *Katz* was the governing case, but it narrowed the Fourth Amendment issue to the following:

> But in *Katz* the Court also stressed that "(w)hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." We must examine the nature of the particular documents

constitutional sense only if it addresses a totally different question: On balance, should society protect the privacy of information disclosed in such a fashion?[118] This prong, in other words, forces the courts to decide whether it is in society's interest to extend the zone of privacy even to protect confidential disclosures. The Supreme Court somehow lost sight of this issue and turned *Katz*

> sought to be protected in order to determine whether there is a legitimate "expectation of privacy" concerning their contents.

U.S. v. Miller, 425 U.S. 435, 442 (1976) (citations omitted). The Court then concluded:

> All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business . . . . The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.

Id. at 442-43. *Smith* adopts a similar approach:

> The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as "reasonable," . . . —whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances.

Smith, 442 U.S. 735, 740 (1979) (citations omitted).

> The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

Id. at 744-45 (citation omitted).

[118] This is the only reasonable reading of the above quoted statement that a caller who takes the precaution to call from a phone booth with the door closed is entitled to the protections of the Fourth Amendment. *See supra* note 91, at 22 & accompanying text. *But see Smith*, 442 U.S. at 740 (converting the inquiry simply to an objective inquiry into risk assumption: "The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'" . . . —whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is 'justifiable' under the circumstances").

into a test that eliminated the issue of societal interest, the only appropriate constitutional concern. The result is a mere tort-like foreseeability test: Information is private only if the Consumer could not foresee its disclosure by a Collector.

The difference between *Katz* and *Katz*-as-interpreted-by-*Miller-Smith,* is far from merely semantic. *Katz* does not direct courts to analyze whether a disclosure was foreseeable, as *Miller-Smith* suggest, but to determine whether information falls within a definition of "private." Whereas *Miller-Smith ipso facto* deny Fourth Amendment protection simply because the Consumer could foresee the risk of disclosure, *Katz* requires the court to evaluate the facts to determine whether the information remains private under the Fourth Amendment despite disclosure. Under *Katz,* the court should consider (1) whether the Consumer has bargained for a promise not to disclose the information to the public or Government, (2) whether the Collector ever actually sees the information, (3) the nature of the information, and (4) the societal benefits of the Consumer's disclosures to the Collector. Under *Miller-Smith* those facts are irrelevant, but under *Katz*, they are relevant to both of the prongs.[119] The first three of the four facts are relevant to the first prong because each is relevant to an expectation whether the Collector would disclose the Data: A reasonable Consumer could have a subjective expectation of privacy because a Collector is certainly less likely to disclose Data that (1) it has promised to keep confidential, (2) it never sees, and (3) the Collector would appreciate is private because of the nature of the information (e.g., health Data). All four facts fit more appropriately into the second prong because (1) society has an interest in enforcing bargains, (2) a mere transfer of Data is not a disclosure that justifies Government access, (3) information that is inherently personal is more worthy of societal protection, and (4) society has an interest in fostering technology and increasing economic efficiency.

---

[119] The *Katz* test might be less subject to misapplication if its two prongs were labeled "individual" and "societal" rather than "subjective" and "objective."

2. A Compilation of Digital Data Is Not the Equivalent To A "Disclosure" of Information

Miller and *Smith* also erred in devising notions of disclosure based on a comparison of personal communication to the transfer of data. The reasoning in both *Smith* and *Miller* relied on cases such as *United States v. Hoffa*[120] that dealt with verbal disclosures by one individual to other persons.[121] In *Hoffa,* the Court held that, although the Fourth Amendment protects citizens from unwarranted government intrusions into their homes, offices and hotel rooms,[122] it does not protect them from their misplaced belief that those in whom they confide will not share their confidences with the authorities. [123]

There is, however, a constitutionally significant factual distinction between *Hoffa* and Government access to stored digital transaction data. In the former situation, the individual who communicates with another person (i) knows what he has said, (ii) knows that the recipient is not only able, but likely, to evaluate the implications of the information transmitted, and (iii) knows that the recipient may decide, based on that evaluation, to disclose the information to others. The one who shares information with another individual is also likely to appreciate and rely on the limits of human memory and the cognitive constraints sociologists call "bounded rationality." The person who shares information also is likely, as a matter of empirical reality, to have some idea of what other information the recipient can combine with the information transmitted.[124]

---

[120] 385 U.S. 293, 301-302 (1966). *See also* Lopez v. United States, 373 U.S. 427, 437-40 (1963).

[121] *Hoffa*, 385 U.S. at 301-02.

[122] *Id.* at 301.

[123] *Id.* at 302 ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

[124] For a discussion of the legal implications of the limits of the human mind to absorb and correlate information, see generally Melvin A. Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 STAN. L. REV. 211

Now, contrast that scenario with the transfer of transactional data in even a simple Internet purchase, such as buying a book from Amazon.com. Because she does not knowingly interact with another human being, the Consumer who buys the book has little reason to believe that a human being will ever observe or evaluate the transaction data. Moreover, depending on her computer expertise, she may fail to appreciate the precise Data that is transmitted and is equally unlikely to have any appreciable understanding of how the Data can be sliced, diced and mixed with other data in the Collector's database.[125] In other words, it is simply not reasonable to conclude that a Consumer who is not well versed in computer technology would view a transfer of digital information as presenting the same risk of a disclosure to Governmental authorities as a verbal conversation with a confidante. Nor would such Consumer be able to appreciate the extent to which the Collector and Government can aggregate the data deriving from a discrete transaction with the Collector with information totally unrelated to the transaction. It is, therefore, simply not "reasonable" to conflate the two scenarios and assume that any online transfer of data is a disclosure of the type addressed by *Hoffa* and analogous cases.

How can we reconcile this conclusion with the holdings in *Smith* and *Miller*? As to *Smith*, the facts are certainly more analogous to the transactional transfer of data described in the preceding paragraph than they are to the "snitch" scenario that provided the factual foundation for *Hoffa.* We might attribute the holding in *Smith* to the fact that it was decided almost three decades ago, at a time when members of the Court were

(1995).

[125] For example, a Consumer who acquires smart house technology may do so primarily for security reasons. She might not be aware of the extent to which real time Data is transmitted and retained by the Collector, nor might she comprehend how that Data can be aggregated with information about utility and telephone usage to provide a comprehensive picture of the activities within the house. It is, of course, the very people who are most unsophisticated about computer technology who are most likely to under-appreciate the extent to which their use of the technology could eliminate their Fourth Amendment rights.

presumably unaware of the potential for, and consequences of, mining data from transactions mediated by evolving technologies.[126] But one member of the *Smith* Court, Justice Marshall, saw the majority's error all too clearly.

> Implicit in the concept of assumption of risk is some notion of choice . . . . [I]n the third-party consensual surveillance cases, . . . the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications . . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance . . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.[127]

Furthermore, just two years prior to the *Smith* decision, the Privacy Protection Study Commission had issued a report that pointed out the dangers of allowing unfettered government access to data held by third parties.[128]

---

[126] The precursor of the Internet existed when *Smith* was decided, but it had not yet permeated popular culture; that process began with the introduction of personal computers in the early 1980's. *See*, *e.g.*, "ARPANET," Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/ARPANET; Eric S. Raymond, *A Brief History of Hackerdom* (2000), http://www. hackemate. com.ar/hacking/eng/ part_00.htm#toc3.

[127] *Smith,* 442 U.S. 735, 749-50 (1979) (Marshall, J., dissenting).

[128] *See* PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, Chapter 9 (1977), http://aspe.hhs.gov/datacncl/ 1977privacy/c9.htm:

> Traditionally, the records an individual might keep on his daily activities, financial transactions, or net worth were beyond government reach unless the government could establish probable cause to believe a crime had been committed. If government were merely suspicious and wanted to investigate, such records were unavailable. The legal standards that protected them evolved in a world where such records were almost universally in the actual possession of the individual. Reflecting that reality, the law only barred government from seizing records in the possession of the individual . . . . [T]hat world no longer exists. Third parties . . . now keep a great many records documenting various activities of a particular individual. Indeed, these third parties

It seems, therefore, that the only explanation for the *Smith* holding is that the Court simply erred, presumably because it failed to contemplate the devastating effects that using the *Katz* assumption of risk calculus to assess the constitutionality of data disclosure by third-parties would have upon privacy. Inferential support for this interpretation of *Smith* comes from state court decisions that have rejected its holding.[129]

---

keep records about the individual he would not ordinarily have kept in the past. Records for life and health insurance, for example, are repositories of highly intimate personal data . . . which were virtually unknown until recent decades . . . .

The existence of records about an individual that are not in his possession poses serious privacy protection problems . . . . Record keepers can . . . [and] often do . . . disclose records . . . to government without seeking the individual's approval . . . . A government request made informally through a personal visit to the record keeper or by a telephone call . . . may leave no trace . . . . Even if the individual is given notice and documentation of the disclosure, he has no legal right to challenge the propriety of government access to his records, despite the possibility that the government agent might have been on a "fishing expedition."

Id. (citations omitted).

[129] *See*, *e.g.*, State v. Hunt, 450 A.2d 952, 956 (N.J. 1982):

The telephone caller is . . . entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes. From the viewpoint of the customer, all the information which he furnishes with respect to a particular call is private. The numbers dialed are private. The call is made from a person's home or office, locations entitled to protection under . . . the New Jersey Constitution.

See also People v. Spoerleder, 666 P.2d 135, 141-42 (Colo. 1983).

A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society. When a telephone call is made, it is as if two people are having a conversation in the privacy of the home or office . . . .

The concomitant disclosure to the telephone company, for internal business purposes, of the numbers dialed by the telephone subscriber does not alter the caller's expectation of privacy and transpose it into an assumed risk of disclosure to the government . . . .

We view the disclosure to the telephone company of the number

This leaves *Miller*. How do we explain the Court's holding? We could rely on the theory we advanced above to account for the holding in *Smith*—but *Miller*, unlike *Smith,* did not involve any use of modern computer technology. In fact, since *Miller* was decided during an era where technology had not yet presented the risks to privacy that are prevalent today, its holding may be a direct function of the times in which it was decided. The Court held that Miller lost any Fourth Amendment expectation of privacy by assuming the risk that a bank employee would and could read the information on any one of his checks. The Court cited *Hoffa* for the proposition that one assumes the risk that those in whom she "confides" will share those confidences with the Government.[130]

> dialed as simply the unavoidable consequence of the subscriber's use of the telephone as a means of communication . . . . Any use the telephone company might make of such information for its own internal accounting purposes is far different from governmental evidence gathering.
>
> One's disclosure of certain facts to the telephone company as a necessary concomitant for using an instrument of private communication hardly supports the assumption that the company will voluntarily convey that information to others. Telephone companies are in the business of providing telephone subscribers with the equipment necessary for electronic communication in today's world. The government, in contrast, investigates for the purpose of prosecuting persons for criminal offenses. The expectation that information acquired by the telephone company will not be transferred without legal process to the government for use against the telephone subscriber appears to us to be an eminently reasonable one.

Id. *Accord* State v. Thompson, 760 P.2d 1162, 1166-67 (Idaho 1988).

[130] *See* United States v. Miller, 425 U.S. 435, 443 (1976). The *Smith* Court used the same approach and finds that neither the nature of the data disclosed or the recipient's decisions as to what information to retain or how to collect it are constitutionally significant:

> The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. Under petitioner's theory, Fourth Amendment

Writing in 1976, the *Miller* Court may have operated on the assumption that transacting business with a local bank was sufficiently analogous to communicating with a confidante to support the application of the *Hoffa* rationale. That is, members of the Court who were a product of a distinctly non-technological era may have assumed that when one dealt with a bank, one dealt with a person—with a teller or a personal banker. If you accept this assumption, then it at least becomes conceivable to apply the *Hoffa* assumption of risk calculus to bank records.

There are, however, factual problems with this assumption, even in a non-technological world. For instance, even if a bank employee who was responsible for processing checks in the 1970's had the opportunity to view individual checks, he likely could not have remembered the information on any one check from among the thousands he processed each day.[131] Today, with advances in automation and the increased efficiency of check processing operations, it is unimaginable that a court reasonably could draw

---

> protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls. Calls placed across town, or dialed directly, would be protected; calls placed across the river, or dialed with operator assistance, might not be. We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.
>
> We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate."

Smith, 442 U.S. at 745.

[131] In the late 1980s, one of the authors was general counsel of a bank that processed checks for over 100 other financial institutions. The clerks who processed checks handled such a volume that they essentially performed their tasks in a "mindless" fashion. This appears to have been true throughout the industry. *See* David H. Autor et al., *Upstairs, Downstairs: How Introducing Computer Technology Changed Skills and Pay on Two Floors of Cabot Bank,* Federal Reserve Bank of Boston – Regional Review (2002), http://www. bos.frb. org/economic/nerr/rr2002/q2/upstairs.htm. Moreover, given the volume of checks processed and the number of processors, it is highly unlikely that any bank employee even saw a significant percentage of any Consumer's checks.

the *Miller* inference.[132]

There are also conceptual problems with the *Miller* holding. The *Miller* result is flawed even if we accept, for purposes of analysis, the empirical assumption that clerks read and remember bank records. Engaging in financial transactions with a bank, even when the bank is represented by an individual, is not analogous to "confiding" in another human being. The structure of the transaction differentiates it from the type of face-to-face interaction at issue in *Hoffa.* Miller's transfer of information did not create the risk of disclosure to Government; it was, rather, the bank's retention, compilation and sorting of that information that permitted Government to obtain useful information about Miller. To phrase the principle more generally, the Consumer has not "disclosed" the information that eventually ends up in Government's hands. It is, instead, the Collector's compilation and sorting of Data that "discloses" usable information to Government.

3. Disclosure To One Party In A Relationship Is Not Disclosure To the Public

Even if we assume, *arguendo*, that a transfer of digital information is a "disclosure" in the *Katz* sense, the *Miller-Smith* approach still conflicts with a historically grounded judicial interpretation of the Fourth Amendment. The *Miller-Smith* opinions implicitly assume that a disclosure to a trusted, reputable Collector is the same as indiscriminate disclosure to the public.[133] While that assumption might follow from an analysis premised on the mere presence of theoretical risk, it ignores the societal value of well-placed trust. That is, society does not benefit from trust

---

[132] *Id.* From the authors' description of the actual processes conducted by employees, it is clear that employees today have neither the time nor any reason to assimilate or aggregate information on individual transactions or across transactions.

[133] *See Miller*, 425 U.S. at 442 ("[I]n *Katz* the Court . . . stressed that '[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'") (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

among thieves (the *Hoffa* situation), but it does benefit from trust among the parties to legitimate personal and commercial transactions. A society that encourages or at least respects trust in these situations enables the Consumer to enjoy the benefits of new technologies without fear that information that would not otherwise be "capture-able" will be appropriated by the Government. Encouraging and respecting trust also allows Collectors to offer those technologies at lower prices because Consumers do not have to negotiate additional protections nor do Collectors have to provide assurances beyond mere trustworthy undertakings.

Neither the *Miller* nor the *Smith* Court explained why any disclosure is equivalent to a public disclosure, even though the logical inconsistency of this proposition is apparent. Public disclosure forfeits Fourth Amendment protection because it eliminates any possible claim that Government intrusion has affected a Consumer's privacy interests. There is far less harm in letting the Government access information the Consumer has shown she has no interest in keeping from anyone. The Government should not be put in a position inferior to that of the general public; what is available to "the public" should also be available to the Government without its having to satisfy the requirements of the Fourth Amendment. So, we cannot raise Fourth Amendment objections if the Government obtains information we post on a publicly-accessible website, displayed in our front yards or discussed in loud voices while on cell phones in a crowded airport. In each of these situations we have clearly demonstrated our lack of interest in controlling access to the information in question. In each of these situations, we have also broadcast the information by knowingly or recklessly sending it into the public domain.

The conduct at issue in these and other broadcast scenarios is vastly different from the conduct involved in, for example, (i) disclosing information to a Collector over a secure Internet connection in the course of purchasing sexual dysfunction medicines, pornography or religious literature and/or (ii) disclosing information as an incident of utilizing the services of an ISP, a

telephone company or a company that provides security or other monitoring services to one's home or office.[134] The disclosures in categories (i) and (ii) are *controlled* disclosures, in that they represent the limited, focused sharing of information with a Collector as an integral part of a legitimate transaction between the individual and that Collector.[135] In that sense, disclosures of this type are more analogous to communications encompassed by evidentiary privileges than they are to the "broadcast" disclosures described in the preceding paragraph.[136]

By failing to appreciate the difference between "broadcast" disclosures and controlled disclosures, *Miller* and *Smith* oversimplify the privacy equation in a fashion that erodes Fourth Amendment protections. The Court should therefore overrule the *Miller-Smith* "*per se* public disclosure" rule and implement a Fourth Amendment standard that protects a Consumer's controlled disclosure of information to a Collector as a reasonable incident of a legitimate transaction for goods or services. Fourth Amendment privacy should not be lost when the event that "frustrates" the Consumer's expectation of privacy is Government's action, including its purchase of Data for surveillance or investigatory purposes, its use of regulatory leverage, or its ability to induce disclosure by a *quid pro quo* bargain arising out of its investigation of the Collector.[137]

---

[134] The fact that a professional athlete proclaims his use of a sexual dysfunction product does not establish that society should decline to regard the transaction noted in the text above as worthy of Fourth Amendment protection. The same holds for the purchase of non-obscene pornography or religious literature, both of which are protected by the First Amendment.

[135] We would not, as noted earlier, bring the *Hoffa* "snitch" scenario into the Fourth Amendment calculus. For one thing, society has no interest in protecting trust in such relationships. For another, the communications in "snitch" scenarios intrinsically involve unlawful activity, unlike the legitimate transactions discussed in the text above.

[136] *See*, *e.g.*, EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE, EVIDENTIARY PRIVILEGES §1.2.1 (2002) ("Recognition of evidentiary privileges . . . promotes personal autonomy in the sense of decisional privacy.").

[137] *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("The Fourth

4. The Assumption of Risk Doctrine Ignores the Consumer's Bargain With the Collector and Her Lack of Meaningful Choice

For the *Miller-Smith* assumption of risk principle to make sense, the following conditions would have to exist: (1) the Consumer did not secure the Collector's promise not to disclose certain information to Government; and (2) at the time she made the disclosure, she had a realistic, practical choice either to (a) reveal that information and forego privacy or (b) not disclose the information and retain privacy. Regarding the first condition, it perverts the English language to say that a Consumer assumed the risk of disclosure when she entered into a transaction with a Collector who promised to maintain the confidentiality of data she provided by the Consumer, either as part of a basic service agreement or website terms of use.[138] Instead, the Collector has

---

Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated."). The authorities should not be able to rely on the "frustration" they have caused. A more difficult issue might concern the ability of Government to use Data a Collector freely discloses albeit in violation of the Collector's confidentiality agreement. One could argue that this is just a variant of the *Hoffa* snitch scenario and the Government should be able to take advantage of the Collector's unilateral decision, thereby leaving the Consumer with her civil remedies against the Collector. We believe, however, that Government should not be able to use that Data because the privacy interest is "shared" and therefore not the Collector's to disclose unilaterally.

[138] Websites vary in how they address the privacy of information. Google for example, has a fairly weak statement of privacy. *See* Google Privacy Policy Highlights, http://www.google.com/privacy.html. Banks, on the other hand, are more likely to warrant greater privacy protection, given the more sensitive nature of the Data they typically collect. *See* Bank of America Privacy Policy for Consumers, http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr ("For example, Customer Information may be disclosed in connection with a subpoena or similar legal process, fraud prevention or investigation, risk management and security, and recording of deeds of trust and mortgages in public records."). Of course, given the current state of the law, Collectors may feel free to carve out from their privacy pledge government requests for Data. *See*, *e.g.*, Insure.com Privacy Policy, http://www.insure.com/privacy_statement.html. The same argument applies when a Consumer transacts business with a website that advertises that it is

assumed the risk of maintaining privacy. Allocating the risk to the Consumer gives the Government an incentive to see that the Collector breaches its agreement with her; this, in turn, would only encourage Government to abuse its leverage as a regulator and prosecutor, something which some suggest is already occurring.[139]

---

certified as maintaining consumer privacy. *See*, *e.g.*, Insure.com Home Page, www.insure.com (promoting that the website is secure by including a logo stating that it is a "VeriSign Secured Site"). Certifications would be an efficient substitute for detailed contractual provisions. Recognition of Fourth Amendment protections for data covered by a confidentiality agreement under the approach urged here would create a market for such certification programs.

[139] *See*, *e.g.*, AMERICAN CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY 10-11 (2004) [hereinafter ACLU, THE SURVEILLANCE-INDUSTRIAL COMPLEX].

> To obtain information about individuals' activities, the government often need do no more than ask. Many companies are willing to hand over the details of their customers' purchases or activities based on a simple request from the FBI or other authorities. Some companies believe they are being patriotic; others may be afraid to turn down 'voluntary' requests because they fear regulatory or law enforcement scrutiny of their own activities; others may simply be eager to please.
>
> Multiple airlines have admitted turning over the records of their customers' travels to the government. In each case, the information was turned over not to help the government solve a particular crime or track a particular suspect, but in order to examine each traveler's records in the hopes of identifying terrorists by detecting 'suspicious' patterns in his or her travels – in effect, turning every traveler into a suspect.

Id.

> Scuba shops. In May 2002 the Professional Association of Diving Instructors voluntarily provided the FBI with a disk containing the names, addresses and other personal information of about 2 million people, nearly every U.S. citizen who had learned to scuba dive in the previous three years.
>
> Colleges and universities. A 2001 survey found that 195 colleges and universities had turned over private information on students to the FBI, often in apparent violation of privacy laws; 172 of them did not even wait for a subpoena.
>
> Travel companies. A 2001 survey of travel and transportation companies found that 64 percent had provided customer or employee

The *Miller-Smith* assumption of risk principle is based on the Court's holding in *Hoffa* that individuals accept the risk of disclosure of their criminal plans.[140] *Hoffa* is, however, factually and conceptually inapposite to the Consumer-Collector relationship. For one thing, Hoffa, who made the disclosure, did not bargain for confidentiality or have any reason to repose trust. Indeed, the opposite is true—a reasonable person would have had every reason to distrust the faithfulness of his criminal associate. The criminal relationship is distinguishable from the relationship between the Consumer and the Collector with whom she transacts business in the ordinary course in reliance on the Collector's assurances of confidentiality. In the snitch scenario, the person is clearly taking "unreasonable" chances; in the Consumer-Collector relationship, the Consumer is simply acting as a rational, law-abiding person operating in a market economy. Also, we must not underestimate the coercive force of a Government "request" to a Collector for information about a Consumer.[141] Even if the Collector is not a directly regulated entity such as a bank or insurance company, legitimate businesses will feel pressure to cooperate with law enforcement requests for information for a variety of reasons,[142] not the least of which is the Collector's need for cooperation from law enforcement in the event that it becomes a victim of cybercrime.

The lack of meaningful choice also distinguishes the Consumer-Collector relationship from the snitch scenario that produced the holding in *Hoffa*.[143] Nothing in the history of the Fourth Amendment suggests that citizens should have to choose between their constitutional rights and access to the most efficient means of participating in commercial and personal affairs.[144] Yet

---

data to the government, many of them in violation of their own privacy policies.

Id. at 11 (notes omitted).

[140] *See infra* Part II.B.2.

[141] *See* ACLU, THE SURVEILLANCE-INDUSTRIAL COMPLEX, *supra* note 139.

[142] *Id*.

[143] *See infra* Part II.B.2.

[144] Indeed, a concern for protecting business and commercial premises was

the ever-increasing pervasiveness of technology, the growth of electronic commerce and the developments in database technology mean that citizens accessing such basic services as communications and banking jeopardize their Fourth Amendment protections just by acting as rational Consumers.

The Court essentially conceded as much in *Smith,* when it recognized that Government could not destroy subjective expectations of privacy by televising notices that citizens were subject to warrantless search.[145] *Miller* and *Smith* effectively constitute such a notice: use a bank or a phone and you lose your Fourth Amendment privacy. In a society marked by ubiquitous technology, the choice to share or not share Data is meaningful only to the Consumer who is willing to forego participation in that society. *Miller* and *Smith* simply reached the wrong conclusion. At the beginning of the twenty-first century it has become apparent that it is not prudent to hold Consumers to a Hobson's choice between enjoying the benefits of modern technology and foregoing their privacy, or becoming Luddites and retaining a level of

---

one of the factors that prompted adopting of the Fourth Amendment. *See* Marshall v. Barlow's, Inc., 436 U.S. 307, 311-12 (1978).

[145] *See* Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979).

> Situations can be imagined, of course, in which *Katz*'s two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country . . . erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.

Id. What we propose in this article is just such a "normative inquiry."

privacy.

5. The Doctrine Encourages Economic Inefficiencies by Ignoring Societal Interests in Privacy and In the Promotion of Technological Advances

Through their legislatures, Americans have expressed an abiding interest in maintaining the privacy of stored transactional data. Recent statutes such as the Gramm-Leach-Bliley Act[146] and the Health Insurance Portability and Accountability Act of 1996[147] include extensive privacy protection provisions. This concern over privacy of stored data is also demonstrated by the massive grass roots objections to a "know your customer" regulation proposed by the federal banking agencies in 1999. More specifically, this legislation has generated tens of thousands of written objections from the public.[148] Thus, it is clear that the American public perceives as reasonable an expectation that Collectors will maintain the confidentiality of their stored data. Clearly, Americans do not assume that permitting Collectors to maintain extensive databases of information gives the Collector the right or power to disclose that information as the Collector wishes. Therefore, denying Fourth Amendment protection simply because the Collector bows to Government pressure[149] to release the information can only jeopardize the confidence of Consumers in the Collectors' undertakings that involve confidentiality.

Jeopardizing that confidence is bad policy for two reasons. First, it will cause Consumers to be less likely to share information, which will result in less reliable information being

---

[146] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801 (2005) (protecting privacy of non-public personal information provided by consumers to financial institutions, especially with respect to disclosure to other commercial entities).

[147] Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. § 164.512(e) (2005) (protecting privacy of non-public personal health information held by doctors, hospitals, insurers, benefit plans and others).

[148] *See* Withdrawal of Notice of Proposed Rulemaking, 64 Fed. Reg. 15310 (Mar. 31, 1999).

[149] *See* ACLU, THE SURVEILLANCE-INDUSTRIAL COMPLEX, *supra* note 139.

provided to Collectors and therefore, less efficient service by vendors. Because this chilling effect is likely to be random, depending as it does on the sensitivity of particular Consumers to privacy issues and the nature of the goods or services provided by the Collector, Collectors will be unable to make accurate adjustments to their Data, and there is likely to be a net loss in Consumer economic welfare.

Moreover, application of the current *Miller-Smith* assumption of risk doctrine to Government requests to Collectors for information will tend to discourage technological advance. First, Collectors' compliance costs will increase on the reasonable assumption that Government requests for information will be broader and more frequent than they would be if Government had to obtain a warrant. Second, some Consumers will forgo the use of technology that involves data retention because they value their privacy more than any time or costs savings associated with the technology. We suggest that there is little policy basis for the Court to adopt a rule that makes Fourth Amendment protection depend on the economic considerations involved in a Consumer's choice to buy pornography at a brick and mortar store instead of over the Internet, especially when we consider the cost savings generally inherent in electronic commerce.

In sum, the *Miller-Smith* approach represents flawed constitutional analysis, unsound economic policy, and harmful social engineering. The Court's formalistic view of privacy, which turns on an un-empirical, non-conceptual notion of assumption of risk, rewards Government for lazy investigation while chilling citizens' willingness to take advantage of the efficiencies and conveniences of new technologies. A non-zero-sum approach to privacy that derives from relationships created to take advantage of new technologies and that is analogous to old-century notions of privacy would be more consistent with Consumer expectations while minimally interfering with Government's ability to conduct appropriate investigations.

III. RELATION-BASED SHARED PRIVACY

The reasoning set forth in Section II leads us to the conclusion that Fourth Amendment protection should not depend on a legally-formalistic assumption of risk model. Instead, we believe that it is more consonant with the purposes and history of the Fourth Amendment for constitutional protection to turn on the nature of the relationship between Consumers and Collectors. The question should be whether the parties have entered into a relationship that demonstrates an intent to share the Data, thus giving each party an independent constitutional interest in keeping that Data private. Stated differently, we contend that Fourth Amendment protection for Data should depend on whether the general purposes that lead (1) Collectors to store and mine it and (2) Consumers to permit that storage and manipulation, reflect the parties' legitimate expectation that the Collector will not exercise sole dominion over the Data. Whether this shared-privacy interest exists is determined from the nature of the transactions involved and the expressions of the parties regarding their relationships.

This model derives not from the language of the Fourth Amendment, for Fourth Amendment analysis is derivative in the sense that the Amendment protects, but does not create, privacy interests. Nor do we draw our analysis from legal principles, although it does bear similarities to traditional property analysis (e.g., the notion that different parties can share ownership interests in the same thing), and traditional contract analysis (e.g., that parties' reliance interests are worthy of legal protection because honoring reliance encourages commerce and discourages unjust enrichment).

We call the approach we derive from this analysis "relation-based shared privacy." In this section, we define the types of relationships and the nature of the privacy expectations that should produce a Fourth Amendment expectation of privacy for stored transactional data maintained by a Collector. Next, we identify four parameters for determining whether Data should be subject to Fourth Amendment protection. Each parameter derives from the underlying competing interests balanced by the Fourth

Amendment: the Consumer's privacy interest in the information and Government's need for it.

We start with the premise that one can share information without contemplating that the information will be disclosed to the public or even to other third persons. We do not suggest, however, that Government should have to inquire on a case-by-case basis into either the subjective or objective intent of parties who disclose information. Rather, Fourth Amendment protection can be based solely on the existence of defined relationships from which we can conclude that society does or should recognize a privacy interest. For example, if we look to old-century analogs, we see that society has long recognized that many of these disclosures take place in the course of defined relationships, such as wife/husband, patient/doctor, client/attorney, and penitent/priest, where society's interest in maintaining the free flow of information justifies even an evidentiary privilege. We also can identify other relationships that have enough societal significance, if only from the viewpoint of personal autonomy and economic efficiency, to justify protecting the disclosing party's interest in the confidentiality of the information even if society does not recognize that the information should be privileged from disclosure in court proceedings. Trade secret protection and enforcement of confidentially (non-disclosure) agreements are just two examples of doctrines that recognize "shared privacy" interests.[150]

In other words, the existence of a relationship of a given nature can demonstrate that the disclosing party expected that the information disclosed would be kept confidential and that her expectation was reasonable. Absent the relationship, the information would not be private. For example, a conversation

---

[150] Of course, the notion of shared privacy does not depend on the existence of express confidentiality agreements. For example, when servants in the home were more common, it would be unreasonable to conclude that the presence of a servant destroyed the privacy of a conversation between family members. The servants understood that a condition of their employment was that the conversations stayed in the room. It would make no sense from a societal viewpoint to hold that a conversation was not private just because family members failed to dismiss the servant from the room before conversing.

between a husband and wife in front of a butler serving dinner in the family dining room would remain private, while the same conversation in the presence of a waiter in a restaurant would not, in the absence of other circumstances, be private.[151]

We conclude that the Fourth Amendment should apply to Data maintained by a Collector with respect to a Consumer under the following conditions:

> (a) the Consumer has provided, and the Collector has collected and retained, the Data in the course of a relationship that permits a reasonable inference that the Data would not be practicably available but for the Data collection and mining capabilities of "pervasive technology;"
>
> (b) the Collector maintains the Data (i) at least in part for the direct benefit of the Consumer and (ii) the Consumer has direct access to at least a material part of the Data;
>
> (c) the Collector has agreed not to disclose the Data to third parties without the Consumer's consent; *and*
>
> (d) Government fails to demonstrate that it could have obtained the Data, independent of a request to the Collector, in the course of employing its own reasonable and ordinary techniques undertaken in connection with the

---

[151] We see two key differences in the two situations. First, the first conversation takes place in the home, where there is a greater expectation of privacy. However, this spatial consideration does not apply to the present context. The more important difference for present purposes is that the spouses have an existing relationship with the butler based at least in part on the trust that the butler will respect the confidentiality of family conversations. In other words, the nature of the trust is that neither the spouses nor the butler feels that the butler is free to disclose the conversation outside the home. This conclusion is based on the historic understanding that the privacy of the home encompassed family members, servants and guests. *See*, *e.g.*, Oysted v. Shed, 13 Mass 520, 522-23 (1816).

No such trust relationship exists with the waiter at least in the absence of other circumstances. The situation might, we repeat might, be different if, for example, the spouses are regular customers of the restaurant and the waiter is their usual waiter who is familiar with their habits.

investigation of a specific crime.

A. Relation-based

Ubiquitous technology requires a re-evaluation of the appropriate balancing of private and public interests for Fourth Amendment purposes. Government should have access to Data that the Consumer has set adrift in the stream of commerce in the sense that the same information would have been disclosed to casual observers or employees of the Collector in comparable real-world transactions. On the other hand, the mere fact that a Collector possesses Data should not enable Government to obtain it. The problem lies in attempting to identify the factors that should be taken into account in determining the appropriate balance in cases between these two extremes.

One way to determine the application of the Fourth Amendment in the world of pervasive technology is to compare such technological transactions with analogous real-world transactions. For example, one factor to consider is the "visibility" or "publicity" of the transaction that created the Data at issue. The Consumer who buys an automobile tire at a retail store has no expectation that the fact of her purchase is private because the seller's employees and other customers can see the purchase; also, anyone seeing her car can infer that she had purchased that brand of tire.[152] The fact of the purchase, therefore, is not private in any sense. Thus, the tire purchaser cannot complain if Government obtains Data from the retail store, or from manufacturer, confirming the fact that she bought that tire or from obtaining related transactional Data such as the time, date and price of the purchase.

The same rule should hold true of Data identifying a single transaction in the pervasive technology world if sufficient indicia identifying that transaction are inherently public. For example, Data regarding a tire purchase does not become private just

[152] *See*, *e.g.*, United States v. Knotts, 460 U.S. 276, 281-83 (1983) (holding that it is not considered a "search" to use a beeper to track someone's movements in public spaces).

because the purchaser completes the transaction in the privacy of her home through cheaptire.com and puts the tire on her car in her own garage with the garage door closed. Even though she may hide from public view many of the aspects of the transaction, the telltale sign is still visible to the public as soon as she takes the car onto the public streets, so Government should have access to the Data for the same reason as stated above for a retail store transaction, assuming, of course, that it can identify the seller.[153]

Different concerns are present, however, when a Consumer and a Collector each manifest an intention to maintain the privacy of transactions that otherwise might be public. For example, a Consumer who desires to purchase prescription medicine and wishes to maintain her privacy might be entitled to Fourth Amendment protection if she purchases the medicine through a secure website that promises confidentiality and that delivers the medicine in a plain wrapper. The Consumer in this instance is in a sense taking the *Katz* precaution of calling from a closed phone booth instead of a pay phone on a restaurant wall, and her decision to maintain her privacy should be honored for the same reason.

The intention to maintain privacy is readily inferable when a Consumer, in the course of creating or continuing a relationship that anticipates at least the strong likelihood of multiple transactions, provides "personal profile" Data that the Collector combines in a database with transactional Data. Such a relationship can be found in the delivery of "profile Data" to the Collector with an expectation on the part of the Consumer and the Collector that the Collector will combine profile Data with transactional Data.[154] This combination of personal information with the details of multiple transactions creates a corpus of information that

---

[153] Thus, although an on-line purchase may not make the Data *per se* private, it might have the same effect by making it impracticable for Government to locate the Collector.

[154] We use "profile Data" to refer to "tool Data" and "Biographical Data" as those terms are defined in *supra* note 40. We emphasize that while each item of profile Data may be public in some sense (e.g., Social Security number, weight, birth date, mother's maiden name) they it can be private when aggregated.

bystanders could not observe and thus supports a conclusion that the Consumer and Collector have entered into a private relationship.[155] Moreover, the Consumer's willingness to allow the Collector to combine personal and transactional Data into a database allows us to infer that the Consumer reposes enough trust in the Collector's goods or services that she anticipates repeated dealings with the Collector.[156] The combination of a corpus of complex information and the prospect of repeated dealings is sufficient to create and sustain a Fourth Amendment expectation of privacy; it also creates the possibility that an aggregation of Data can compromise Consumer privacy.[157]

---

[155] For example, it would not be reasonable to expect that any observer of my purchase at Wal-Mart on a given date could keep track of everything I purchased and associate that with my name and credit card number, much less combine that Data with other Data available to Wal-Mart in its database such as details of my other purchases over the years, warranty claims, and information derivable from credit-reporting agencies obtainable with my credit card data such as address. In other words, by shopping at Wal-Mart I have allowed a collection of Data to exist that would be incredibly expensive, if not impossible, to obtain through traditional eyewitness observation.

[156] The trust we refer to is not trust that the Collector will not disclose information. Rather, it is the Consumer's trust in the value of the Collector's products such that the Consumer anticipates continued dealing with the Collector. It is this trust that makes the Consumer's disclosure of Data to the Collector reasonable under the second prong of the *Katz* test. *See supra* note 103 & accompanying text.

[157] Note that the Consumer may have an expectation of privacy even if such Data pertained to a transaction occurring outside the context of pervasive technology. For example, mail order and phone order transactions are not observable by third parties any more than Internet transactions, and the records maintained by the Collector may not differ between the two types of transactions. To the extent that database technology is employed in such "old-world" transactions, our argument, as set forth below, may apply to those transactions as well because Consumers should be encouraged to participate fully in modern society without requiring a forfeiture of constitutional protections. We also note that drawing distinctions in any of these types of transactions based on comparisons of database contents to the potential recollections of Collector employees is not persuasive, especially when transactions are completed solely on the basis of digital transmissions and computer generated documents and records. For example, given computer

Why should the existence of a relationship with no legal substance or grounding have Fourth Amendment significance? The answer to that question requires us to revisit the notions of privacy discussed previously in Section I. Pervasive technology changes the focus of privacy from a Consumer's right of physical control over space or tangible property into a right to impose economic sanctions for disclosure of information in databases over which the Consumer has no physical control or access. While the notion of physical control is a reasonable approach to implementing Fourth Amendment privacy when we deal with spaces and things, it is meaningless with respect to a modern information-based economy. The very nature of an information-based economy depends on the transfers of information, and to that extent the maintenance of exclusive control renders information valueless. As a result, commercial parties virtually always require a transferee of "proprietary" (i.e. non-public) Data to execute a "non-disclosure agreement."[158] If commercial parties with substantial resources at stake cannot insist on physical control over Data, it is difficult to imagine how any good faith application of the second *Katz* prong requires such control. That is, the practice demonstrates that society is prepared to respect privacy claims as to information even when the claimant has failed to retain physical control or access. Requiring physical control, therefore, would effectively place Data beyond the Fourth Amendment without any balancing of societal costs. In short, neither control nor rights of physical access can provide a limiting principle that will distinguish Fourth Amendment-protected interests in Data. Instead, we need a surrogate that will enable us to avoid both the total abrogation of the Fourth Amendment to Data in a world of pervasive technology and an unprincipled *ad hoc* application that turns on mere

---

technology, no employee even completes an address label. This distinction is no less meaningful because it was not credited in *Miller,* where the Court found a disclosure even though there was no showing (and little likelihood) that any bank employee had or realistically could have had any knowledge of the information contained in the bank's records.

[158] *See* Raymond T. Nimmer*, Images and Contract Law—What Law Applies to Transactions in Information*, 36 HOUS. L. REV. 1 (1999).

formalistic notions of privacy.

Focusing on the existence of a "trust" relation between the Consumer and the Collector, even though the trust may be merely inferential and minimal, enables us to evaluate the reasonableness of a Consumer's claim that Data remains private. This is true even though the Data is being maintained by a Collector in a format easily accessible upon Government request. Prior to the implementation of pervasive data collection, retention and aggregation technology, there was not a realistic possibility that a Collector could disclose Data reflecting a Consumer's personal profile information and the details of numerous specific transactions between the Consumer and the Collector. We can therefore confidently say that Consumers in most circumstances had a reasonable, empirically-based expectation that the aggregate Data reflecting those transactions was not available to Government. When the Consumer "trusts" the Collector and its products enough to anticipate the potential for such aggregation of information, it is unreasonable to conclude that the Consumer in providing Data is indifferent to its use. In a very real sense the trust in the Collector's products reflects trust in the integrity of the Collector to maintain the privacy of the Data provided.[159]

Unless we are ready to adopt the view that Fourth Amendment protection should continually narrow as technology increasingly permits information to be stored and correlated, there is little reason to conclude that a Consumer should expect that Data becomes public just because it is mined and aggregated. That is, Data inaccessible in the real-world should not lose Fourth Amendment protection just because it can be accessed in the pervasive world. Even if the Data can be readily provided to Government upon request, *Katz* nevertheless counsels that, as a matter of societal values, a Consumer can still reasonably expect that it will not be so disclosed simply because she has chosen to conduct her affairs by using more efficient pervasive technology to conduct transactions with "trusted" parties.

---

[159] *See supra* notes 138-39 & accompanying text for examples demonstrating the prevalence of such Consumer attitudes.

B. Shared Interest Based on Direct Consumer Benefit and Access

Not all Data possessed by a Collector in the course of a "trust" relation will be entitled to Fourth Amendment protection. There is still a role for assumption of risk. A Consumer should be held to have assumed the risk that Data collected at the sole instigation and for the sole benefit of the Collector is beyond Fourth Amendment protection because the Consumer effectively set the Data adrift in the stream of commerce. For example, before the advent of Data mining, businesses collected Data for internal marketing, inventory control, product quality, regulatory and warranty liability purposes. The Collector's use of that Data indirectly benefited Consumers in general, whether by lower prices or higher quality. Usually, however, the Data itself was not manipulated and re-disclosed to assist the Consumer in making additional purchase decisions or obtaining services.[160] Stated differently, individual Consumers received no direct benefit from the collection of the Data. Therefore, one could not reasonably conclude that the Consumer had provided the underlying information with the expectation that the Collector would use the Data for the Consumer's own purposes and benefit. In short, the Consumer had given up any "interest" in the information.

In contrast, Consumers who provide "profile" Data to Collectors generally do so because that profile information, when combined with transactional Data, saves the Consumer time and/or money. A significant amount of those savings can derive from the ability of database technology to aggregate or isolate Data to provide the Consumer with new information or insights regarding her dealings with the Collector. Amazon and eBay are perhaps the most famous examples of merchants facilitating customers purchasing by keeping track of past purchases and items of interest, and by offering suggestions based on profiling information. This practice is now so widespread that the websites of our banks, our electric utility companies, our insurerers and

[160] To the extent the information was so used by salespeople, for example, our notion of shared privacy might apply.

others readily present me with personalized information that greatly reduces my need to keep my own records or to conduct extensive investigations of suitable products. In this context, it seems reasonable to conclude that the Consumer has a shared interest in the Data because Consumers are induced to provide the relevant information at least in part on the ground that it will benefit them as much as the Collector. Because the Consumer retains an interest in the Data, the Collector should not have a unilateral right to consent to disclosure to Government. Moreover, it is reasonable for society to protect that Data from Government access because disclosure would discourage Consumers from sharing Data that allows them to make more intelligent and more efficient transactional decisions. As *Katz* demonstrates, Consumers who take reasonable steps to protect or enhance their privacy do not lose their Fourth Amendment rights just because a party with whom that information is shared decides to disclose it to Government.

This shared interest is particularly evident when the Collector enters Consumer-provided Data into a database that allows the Consumer direct access to information about the Consumer's dealings with the Collector. The right and value of direct access to information regarding past transactions and related financial information is one of the great benefits of Internet-accessible Data mining. For example, by going to "My Account" on a electricity utility's website, a Consumer can review her past electricity usage, compare it to average usage statistics, estimate potential energy saving from replacing her water heater, and evaluate the effect of various pricing options in light of her particular energy usage patterns. Such access permits a Consumer to use the Data for her own purposes unrelated to any benefit to the Collector. For example, a Consumer might consult information on orbitz.com regarding past flights and hotel stays in connection with purchasing travel services on expedia.com or directly from an airline. Therefore, the independent usage strengthens the notion of a shared interest by both the Collector and the Consumer.

Direct access also reinforces the significance of the "relation" element because it demonstrates the existence of a more permanent

relationship between the Collector and the Consumer. The Collector incurs the expense of creating and maintaining the database to increase the likelihood that the Consumer will enter into additional transactions with the Collector. It is this repetition that creates the aggregation of Data that increases the risk of an invasion of privacy and invalidates an analogy to observation of real-world transactions. In short, direct access is a significant limiting characteristic of relation-based shared privacy because it is strong, investment-backed evidence that the Collector and the Consumer are parties not just to a transaction, but to a private relationship.

C. Confidentiality Representation or Agreement

Parties in the world of pervasive technology rely on contractual promises to control access to Data. A Consumer should be required to demonstrate that such a promise existed if she desires Fourth Amendment protection for her Data. Otherwise, her privacy claim is simply not reasonable or credible. Those who do not value privacy enough to satisfy this simple element cannot complain when the Collector complies with a Government request for Data. We do not mean to suggest that Consumers must draft their own confidentiality agreements or even have read, much less fully appreciate, a Collector's "website terms of use" regarding privacy and Data usage.[161] Instead, it is likely that market forces will be sufficient to attract privacy-conscious/valuing Consumers to Collectors who unilaterally represent that they will not disclose Consumer-related Data to Government or third parties without the Consumer's consent. Thus, a Consumer satisfies this element of

[161] One might argue that the Consumer should have to demonstrate knowledge of the privacy undertaking as a condition to satisfying the first (subjective) prong of the *Katz* test. We believe, however, that placing that burden on the Consumer would (i) ignore rational Consumer behavior in relying on the branding efforts of leading merchants and on referrals from friends and others and (ii) impose unnecessary transaction costs (reading such terms) for little societal benefit. In other words, ignorance based on trust should be bliss, until Government shows that the trust was misplaced.

relation-based shared privacy by demonstrating that the Collector included such a confidentiality undertaking in its customer agreement or website terms of use. It should also be sufficient to show that a third party credentialing service has certified that the Collector's privacy procedures include a commitment not to disclose Data to Government without a warrant or grand jury subpoena.

D. Government Need

The final element of the principle of relation-based shared privacy might be understood better as an exception to the general rule established by Subparts A through C. The rule should not apply when its application would only make Government incur unnecessary costs or delays in getting information it could practicably obtain for similar real-world transactions. Therefore, even if a Consumer establishes the first three elements of the principle, Government still should be able to obtain the Data by convincing the Collector to comply with a request if the Government can show it would have uncovered the information contained in the Data by using in good faith its own reasonable and ordinary techniques in the course of a criminal investigation.

For example, a hackneyed Hollywood police investigatory technique involves checking with dry cleaners to determine the possible owner of clothing found at the crime scene. There is no suggestion that the Fourth Amendment prohibits the cleaner from checking its records to identify the laundry mark on a shirt. We do not suggest that a different result should obtain simply because the Collector complies with such a crime-originated request by referring to bar coded laundry marks and Consumer accessible Data on laundry preferences and usage. However, the burden is on Government to demonstrate that it could have obtained the relevant information even without access to the relevant database. Government could satisfy that burden, for example, by showing that the laundry could have provided the relevant information just from Data maintained for its own purposes, even though the Data would have been protected under the first three elements of

relation-based shared privacy. For example, the laundry could disclose information, such as name, address and telephone Data obtained to help it contact customers in case of loss or damage to articles or a customer's failure to pick up and pay for articles cleaned. What it could not do is associate that Data with other Data which it maintained for the Consumer's benefit, such as historical data on cleaning of overcoats.

This "could have obtained it anyway" notion should not be applied too generously, especially in the context of requests for large amounts of Data.[162] Data mining and sifting enable detailed, sophisticated and rapid analysis of data that only a generation ago would have taken a team of investigators months to analyze. Therefore, the exception should not apply simply because the Data requested could have been derived from records, such as individual invoices or meter readings, the Collector "always" maintained. Rather, the exception should apply only if it is reasonable to conclude that (i) a Collector would have complied with a request for the Data in that format and (ii) Government (or the Collector) would have been able to create the Data actually requested within the timeframe and budgetary constraints of the investigation at issue.

The requirement of "good faith" should also be emphasized. In making requests of Collectors, Government should rely on traditional citizen incentives to cooperate with crime investigations. Any use of leverage by Government to obtain "cooperation" by threats or suggestions of unrelated regulatory initiatives or independent investigations of the Collector's own activities does not constitute good faith. Nor should Government be able to rely on promises or threats related to cybercrime protection for the Collector. A Collector should not be put in the position of sacrificing a Consumer's privacy interests to protect the

---

[162] Government requests to Collectors for Data does not raise Fourth Amendment concerns when the Data requested are aggregated and not attributable to specific Consumers. Although Collectors are free to ignore such requests, Government should be able to make the request and use the Data because such Data do not disclose any information that could compromise any Consumer's privacy interest.

Collector's own interests. This likelihood that a Collector will succumb to such leverage is especially great where the Consumer is unlikely to have the resources to enforce its contractual rights of non-disclosure and/or where any enforcement would be futile because of difficulties of proving causation or damages.

Finally, the exception should not swallow the rule—it is intended only to assure that cyber-based Data does not receive more protection than traditional sources of information. There is a great tendency for Government to seek access to Data to determine if a crime has been committed or to identify crime risks. Although such requests may be finely tuned enough that they cannot fairly be called fishing expeditions, there is nothing particularized about them and the comparison to the "general warrant" procedure can be readily drawn. The exception under discussion cannot be used to justify such surveillance-based searches. Once Government shows, however, that its request for Data was made in good faith in the course of the investigation of a specific crime, it should not be precluded from using that Data in prosecution of that crime or other crimes as long as the conditions of the exception are met.

CONCLUSION

History demonstrates that the Fourth Amendment has always been construed to require a balance between two societal interests: Government's need to enforce the law and the citizen's need to be left alone. The appropriate balance may change as our culture changes and as our views of the relative importance of law enforcement and privacy change. Mere changes in technology, however, should not affect that balance unless and until they are incorporated in our culture. The phenomena of pervasive computer technology and data mining and sifting will eventually change our society in fundamental ways, but they are too recent to affect the Fourth Amendment balance. In the meantime, constitutional law should encourage Americans to enjoy the benefits of technological advances without concern that doing so will force them to sacrifice their constitutional rights. Thus, courts should apply the Fourth Amendment on a technologically neutral basis—new technology

should neither *per se* extend nor retract the scope of constitutionally permissible Government intrusions.

We have argued that the pervasiveness of computer and database technology creates significant new risks of Government intrusions into the fabric of our daily lives. The low cost of information retrieval and increasing Government leverage over information Collectors substantially increases the risk that those intrusions will occur beyond the reach of the Fourth Amendment. Although the Supreme Court's decision in *Katz* provided a workable standard for protecting Consumers from Government attempts to take advantage of pervasive technology, the Court's decisions in *Miller* and *Smith* rely too heavily on legalistic concepts divorced from societal interests. As a result, a real danger exists that aggregations of extremely sensitive personal information will be available to Government just for the asking.

We believe that the traditional balance, as reflected in *Katz*, can be retained only if the Court rejects the formalistic "assumption of risk" approach and instead recognizes the privacy interests inherent in aggregations of stored transactional data. We have proposed a principle of "relation-based shared privacy" which distinguishes Data that should be protected because it is in society's interests to facilitate trust-based relationships and efficient sharing of information. By focusing on specific attributes of those relationships while protecting Government's ability to investigate crimes efficiently, our principle assures that Consumers who take advantage of pervasive technologies will not thereby sacrifice their right to privacy under the Fourth Amendment.