The Memory Gap in Surveillance Law

Patricia L. Bellia†

INTRODUCTION

In March 2007, Google announced a change in its data retention policy: that it would "anonymize" search data in its server logs after eighteen to twenty-four months.[1] For many observers, the policy change was more significant for the past practice it confirmed than for the future practice it heralded. The policy change underscored that since it first launched its search service, Google had stored its users' search queries, along with the search results on which the users clicked, indefinitely, and had done so in such a way that this data could be tied to the particular computers from which the queries were made.[2]

Although Google's privacy policy has long stated what kinds of information the company collects and discloses, that policy has never mentioned Google's data retention practices.[3] Nor does US law significantly constrain data retention practices, whether by the data subject herself or by a third party (such as Google) that transacts business with the data subject.[4] Our surveillance and information privacy laws,

† Professor of Law, Notre Dame Law School. I thank A.J. Bellia, Susan Freiwald, Nicole Garnett, John Nagle, Ira Rubenstein, and Paul Schwartz for helpful comments and discussions, and research librarian Christopher O'Byrne for expert research assistance.

1 See Peter Fleischer and Nicole Wong, *Taking Steps to Further Improve Our Privacy Practices*, The Official Google Blog (Mar 14, 2007), online at http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html (visited Jan 12, 2008).

2 More precisely, Google links search information to a persistent "cookie"—a small file containing a string of characters—that uniquely identifies the user's browser. Google transmits this cookie when a user's browser first contacts Google's servers, and the cookie persists until it expires or is deleted. Google sets its cookies to expire in 2038. Adam Cohen, *What Google Should Roll Out Next: A Privacy Upgrade*, NY Times A18 (Nov 28, 2005) ("It is hard to believe most Google users know they have a cookie that expires in 2038.").

3 For the current and past versions of Google's privacy policy, see *Google Privacy Policy* (Oct 14, 2005), online at http://www.google.com/privacypolicy.html (visited Jan 12, 2008); *Google Privacy Policy* (July 1, 2004), online at http://www.google.com/privacy_archive.html (visited Jan 12, 2008); *Google Privacy Policy* (Aug 14, 2000), online at http://www.google.com/privacy_archive_2004.html (visited Jan 12, 2008).

4 For discussion of two sector-specific US statutes that do limit data retention, see note 49. The European approach to data privacy is quite different. The European Union's data protection directive regulates the processing of personal data. The directive regulates the procedures by which a data controller can process data (for example, requiring the controller to notify a supervising authority in the member state of the data processing permitted); the purpose for which the data processing can occur; and the rights of the data subject to access the data and demand rectification, deletion, or blocking of data that is inaccurate or not being processed in accordance

in short, contain a "memory gap": they regulate the collection and disclosure of certain kinds of information, but they say little about its retention. In addition, much of what the law does say about collection and disclosure provides incentives for indefinite data retention.

The law's memory gap has ever-increasing significance for the applicability of the Fourth Amendment's warrant requirement to government surveillance activities. When government agents' direct, ongoing observations of a target's activities would invade a reasonable expectation of privacy, agents ordinarily must obtain a warrant before engaging in those observations. The reasonable expectation of privacy test derives from *Katz v United States*,[5] a case dealing specifically with surveillance to collect the contents of communications,[6] but the test applies to other surveillance activities as well. In *Kyllo v United States*,[7] for example, the Supreme Court applied *Katz* to invalidate agents' use of thermal imaging technology to acquire details about heat patterns inside a home.[8]

Current Fourth Amendment doctrine, however, takes a dramatically different approach to government agents' *indirect*, surveillance-like activities, even when those activities yield precisely the same information as—or more information than—direct observation. More specifically, in its "business records" cases, the Supreme Court has held that the warrant requirement is not implicated when a third party collects information (even under a statutory mandate) and the government then obtains that information from the third party.[9] In *United States v Miller*,[10] for example, the Court held that government did not violate the Fourth Amendment by presenting a subpoena rather than a warrant

with data protection rules. See Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 38 Off J Eur Communities (L 281) 31 (Nov 23, 1995).

5 389 US 347 (1967).

6 Id at 348 (describing the placement of an electronic listening device on a public telephone booth to capture the target's end of conversations). More precisely, the test derives from Justice Harlan's opinion in *Katz*, id at 361 (Harlan concurring) (describing 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'"), which was adopted by the Court in subsequent cases. See, for example, *Smith v Maryland*, 442 US 735, 740 (1979).

7 533 US 27 (2001).

8 Id at 40.

9 See *United States v Miller*, 425 US 435, 440 (1976). See also *Smith*, 442 US at 743–45. The rationale for these cases is that one who conveys information to a third party, even for a limited purpose, assumes the risk that the third party will convey that information to the government. I critique the doctrinal basis for this approach elsewhere. See Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 Geo Wash L Rev 1375, 1397–1402 (2004) (arguing that *Miller* improperly conflated two distinct lines of cases, one involving government access to corporate records and the other involving the risk that third parties with whom one communicates will reveal information to the government).

10 425 US 435 (1976).

to compel a bank to disclose records concerning the defendant's bank accounts—records that the bank was statutorily required to collect.[11]

Because the government can only compel disclosure of that which is retained, the scope of the business records "exception" to *Katz* is deeply dependent on data storage practices, and thus on the legal, technological, and economic forces that drive those practices. As I will argue, current and developing data retention practices threaten to convert many of the government surveillance activities now subject to a warrant requirement into the sort of "indirect" surveillance at issue in—and unprotected by—*Miller*. This threat is perhaps easiest to see in the context of communications surveillance, where shifts in information storage trends may render *Katz* itself (and the statutes built on its foundation) a dead letter.[12] But other data trends are equally significant. Stand-alone products that generate no data are increasingly giving way to third-party services that do; such services will yield a profile of behavior that could otherwise only be assembled with direct surveillance activities.[13] Similarly, the trend toward "pervasive" computing will produce vast amounts of data that is capable of being stored by third parties and that mirrors data government agents could otherwise obtain only via direct observation.[14]

Information held by third parties has always flowed to government agents in some measure, and so it may be tempting to argue that evolving patterns of data storage raise no new doctrinal or normative concerns. From a doctrinal perspective, *Miller* and its progeny hold that one lacks a reasonable expectation of privacy in items that one voluntarily surrenders to a third party, and so the conclusion that data stored in digital form with third parties is outside of the Fourth Amendment's protective core is fairly straightforward.[15] From a normative perspective, if one accepts the business records doctrine (either on first principles or on the view that the doctrine is well entrenched), a principled basis on which to distinguish data in digital form from data in other forms is not readily apparent, particularly if one believes that the law should be neutral as to modes or forms of communication and storage.

---

11 Id at 441.

12 See Part II.A.

13 See Part I.C.

14 See Part I.D.

15 As I argue later, however, that conclusion is less straightforward when it comes to the contents of communications stored by third parties rather than data generated in interactions with third parties. See Part II.A.2. See also Bellia, 72 Geo Wash L Rev at 1403–12 (cited in note 9) (arguing that *Miller* and *Smith* should not be read to suggest that an individual lacks an expectation of privacy simply because information was conveyed to a third party).

I argue that the significance of current and developing data storage trends lies in the shift toward an architecture of increasingly "perfect" memory. Fourth Amendment doctrine has always permitted data to flow from third parties to the government. Importantly, however, that doctrine and the laws that supplement it have also coexisted with technological and economic factors that produce surveillance gaps. The dominant architecture of the predigital era was an architecture of forgetting: data about most of our activities could not be captured at all, could be memorialized only imperfectly, or could be retained long term only at significant cost. As these constraints on memory erode, so too will the zones of information privacy they have supported.

Observing that the shift toward an architecture of perfect memory will have important consequences for surveillance and privacy does not resolve how (if at all) the law should respond to that shift. Put another way, it is not obvious why the law should privilege surveillance gaps and imperfections, even if such imperfections have existed in the past. Indeed, lawmakers seem poised to move in the opposite direction—to mandate rather than curb the retention of data, particularly data concerning communications activity.[16] I nevertheless argue that the law should play a role in blunting the surveillance-enhancing effects of our changing architecture of memory.

I begin in Part I by exploring the trends toward an architecture of perfect memory. In addition to discussing general trends in digital storage, I explore two ongoing trends that change the architecture of digital memory: (1) the pulling of communications and data from network "endpoints," such as a personal computer, into the network itself (and thus from an individual data subject to a third-party data holder); and (2) the trend toward "pervasive" computing, which will involve the generation and storage of massive amounts of environmental and experiential data about day-to-day activities. In Part II, across different categories of data, I explore the divergent legal frameworks that regulate what I call "direct" and "indirect" government surveillance

[16] See, for example, HR 837, 110th Cong, 1st Sess (Feb 6, 2007), in 153 Cong Rec H 1270 (Feb 6, 2007) (proposing a requirement that the Attorney General to issue regulations governing retention of ISP records). The text of this draft bill is also available at http://www.govtrack.us/data/us/bills.text/110/h/h837.pdf (visited Jan 12, 2008). The European Union has adopted a data retention directive obligating member states to adopt requirements that communications providers retain certain categories of traffic data for between six months and two years. Covered data includes information regarding the source, destination, duration, and type of communication, as well as information necessary to identify a subscriber's communication equipment and, in the case of mobile equipment, its location. See Council Directive 2006/24/EC of 15 March 2006 on the Retention of Data, 49 Off J Eur Communities (L 105) 54 (Apr 13, 2006). The data must be retained "in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay." Id at 59.

activities. In particular, I explore how the absence of constraints on data retention, coupled with limited constraints on information transfer, provide incentives for private parties to retain data indefinitely, thereby exposing such data to a weaker legal regime than would apply if government agents sought to acquire the data directly. Finally, in Part III, I consider how the law has responded and should respond to these trends.

I. TOWARD AN ARCHITECTURE OF PERFECT MEMORY

Collections of data about individuals are not new. The rise of networked technology, however, has intensified concerns that collections of data in digital form can be searched, copied, and merged with other data sources to form increasingly complete data profiles.[17] Professor Daniel Solove has written extensively about the development of these detailed databases—"digital dossiers," as he calls them.[18]

The extensive computer databases Professor Solove describes are the product of the dramatic advances in digital storage technology over the last half century, which enable companies to store extraordinary quantities of records compactly and at ever-declining cost. Those companies can include both the entities with which we do business—retailers, telephone companies, airlines—and the intermediaries that facilitate our transactions—banks, credit card companies, ISPs, and so on. In addition, those companies can include database companies with which we have no direct relationship, but that mine for personal data from public and private sources and "rent" such data for marketing and other purposes.

This Part explores how these technological and market trends, as well as other trends I describe below, are changing the "architecture" of memory. Two aspects of this changing architecture are significant. First, digital memory is becoming increasingly "perfect": the low cost of storing vast quantities of data in digital form, and the ease of converting nondigital information into digital form, removes many of the incentives of businesses and individuals alike to destroy data. Second, data previously held by the individual whom the data concerns is increasingly held by third parties—even third parties with whom the data subject has no business relationship.

---

17 See Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan L Rev 1373, 1374 (2000).

18 See Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, 13–26 (NYU 2004); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S Cal L Rev 1083, 1089–95 (2002).

I begin in Part I.A by discussing some of the technology and cost trends in digital storage. I do so in detail in part because a sense of the state of technology at various points in time is useful for evaluating the legal framework, which I undertake in Parts II and III. In Parts I.B and I.C, I then discuss other trends pushing toward an architecture of increasingly perfect memory. In addition to the transactional activities on which Professor Solove focuses, I discuss two other trends: (1) a shift in storage and processing capabilities away from network "endpoints"—such as personal computers—to the center of the network (or of multiple overlapping networks); and (2) trends toward "ubiquitous" or "pervasive" computing.

A. The Technology and Cost of Data Storage

Digital technology is simply one of many in a succession of technologies that enable us to generate, retain, and transmit information more cheaply. Data retention has long been a commercial goal, not to mention a broader collective and individual goal among those seeking to preserve generational memory. Until the last half century, however, the expense of storing, indexing, and preserving access to information has required careful choices between maintaining and purging information.

Developments in data storage technology now make indefinite data retention feasible for businesses and individuals alike. Although these developments are difficult to quantify, I illustrate the shifts in the technology and cost of storage in two ways. First, I examine trends in one type of "low-end" storage medium—the hard drive—which remains the most ubiquitous digital storage medium among consumers. Second, I discuss trends in "high-end" storage by focusing on the re-emergence of a specialized online storage industry.

1. Cost and density trends in hard-drive storage.

Digital technology involves the conversion of data—whether text, audio, or images—into a series of "binary digits" (also known as "bits"), each taking a value of zero or one. Storage of the resulting data is measured in "bytes," a term that in modern computer usage refers to a collection of eight bits. A kilobyte (KB) represents one thousand bytes; a megabyte (MB) represents one million bytes; and a gigabyte (GB) represents one billion bytes.[19] Once converted to digital

[19] The figures in the text and elsewhere in this article rely on the decimal rather than binary sense of the International System of Units (SI) prefixes. Because early computers used binary (base 2) rather than decimal (base 10) addressing methods to access system memory, the SI prefixes traditionally associated with multiples of 10^3 (1000) were instead associated with multiples of 2^{10} (1024). Some confusion remains in this regard, particularly because many operat-

form, data can be stored through many different processes, including mechanical processes (used to mark data on punch cards and paper tape), magnetic processes (used to record data on magnetic tapes, hard drives, and floppy disks), optical processes (used to "burn" CDs and DVDs), and electrical processes (used in connection with flash memory on memory cards or flash drives).

Focusing on the cost and storage density of hard drives gives some sense of how dramatically the cost of storage as fallen, at the same time that storage density has increased dramatically. Magnetic storage continues to be the dominant form of storage for data,[20] and hard drives account for some 50 percent of total magnetic storage capacity shipped each year.[21] IBM introduced the first magnetic hard drive for commercial data storage in 1956. The $50,000 system ($363,600 in today's dollars) consisted of fifty disks, each two feet in diameter, and could store 5 MB of data at a density of two thousand bits per inch.[22] The first commercially available hard drives for personal computers had appeared by 1980. In 1981, Seagate, which would become the world's largest producer of disk drives, marketed its 5 MB hard drive with a diameter of 5.25 inches for $1,700 ($4,010.45 in today's dollars)[23]—for users, a per-megabyte cost of $340. In the mid-1980s, as Congress considered and passed the main statute regulating electronic communications, the per-megabyte cost of hard drive storage remained at $100 ($180.61 in today's dollars). By 1999, the cost had fallen to less than ten *cents* per megabyte, or less than $100 per gigabyte.[24] Hard drive storage presently costs consumers less than $1 per gigabyte.

Meanwhile, developments in magnetic processing have allowed manufacturers to increase the density of stored information and thus to reduce the size of storage devices. The IBM hard drive first introduced in 1956 for commercial data could store data at a density of two thousand bits per square inch. By 1981, data could be stored at a den-

---

ing systems still describe memory in binary terms. For example, an operating system might measure a hard drive marketed as having a 160 GB (or 160,000 MB) as having a capacity of 152,588 MB, with MB here used in the binary sense.

20 See Peter Lyman and Hal R. Varian, *How Much Information? 2003* 1 (Oct 30, 2003), online at http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf (visited Jan 12, 2008) (noting that, for 2002, approximately 92 percent of new information was stored on magnetic media).

21 This percentage was calculated from id at 50–61, using figures for the annual storage capacity of each form of magnetic storage.

22 Geoff Nairn, *Drive to Replace Magnetic Storage*, Financial Times 22 (Apr 20, 1995); *Research History Highlights: History of IBM Research 1945–1998*, online at http://www.research.ibm.com/about/past_history.shtml (visited Jan 12, 2008).

23 Ephraim Schwartz, *Hot Seat; Seagate's Drive; CEO Alan F. Shugart Shares the Storage Giant's Take on NCs and Drive Technology*, InfoWorld 25 (Nov 11, 1996).

24 D.A. Thompson and J.S. Best, *The Future of Magnetic Data Storage Technology*, 44 IBM J Rsrch Dev 311, 312 (May 2000).

sity of more than twelve megabits (or twelve million bits) per square inch,[25] and by the mid-1980s, data could be stored at a density of twenty megabits (or twenty million bits) per square inch.[26] Storage density had increased to 700 megabits (700 million bits) per square inch by the mid-1990s[27] and to approximately 100 gigabits (100 billion bits) per square inch by 2006,[28] an increase over the 1956 density by a factor of 500,000.

To make these capacity and density figures more meaningful, it is useful to relate them to paper storage. If stored in digital form, the text of a single typewritten page would occupy approximately 2 KB of storage.[29] Low-end desktop computers are currently marketed with hard drives with at least 250 GB of storage.[30] A large portion of that storage will in practice be devoted to the computer's operating system and other software, but in theory such a device—typically 3.5 inches wide for a desktop computer—could store approximately 125 million pages of text. The printed collection of the US Library of Congress, if stored as text in digital form,[31] would occupy fewer than sixty-three such storage devices. Storing the equivalent of the US Library of Congress's current printed holdings as text in digital form would have occupied at least twenty-five million square feet of storage in 1956, between thirty thousand and forty thousand square feet in 1981, and less than sixty square feet in 2000.[32]

2. The resurgence of the mass online storage industry.

Although data regarding hard-drive storage and density can give some sense of the overall shifts in the cost and technology involved in storing data in digital form, the picture becomes fuller with a discus-

25 J.M. Harker, et al, *A Quarter Century of Disk File Innovation*, 25 IBM J Rsrch Dev 677, 678 (Sept 1981).

26 Thompson and Best, 44 IBM J Rsrch Dev at 312 (cited in note 24).

27 Id.

28 George Lawton, *Working Today on Tomorrow's Storage Technology*, 39 Computer 12, 19 (Dec 2006) (noting that current hard disk storage densities are 100 gigabits per square inch); Sally Bryant, *Hard-disk Drives: 50 Years and Going Strong*, Solid State Technology S20 (Sept 2006) (reporting a one-inch drive with a twelve GB, or ninety-six gigabit, capacity);

29 See Lyman and Varian, *How Much Information?* at 3 (cited in note 20).

30 The lowest-priced desktop computer available on www.dell.com as of November 4, 2007, was offered with 250 GB of storage. See http://www.dell.com/content/products/productdetails.aspx/inspndt_53xs?c=us&cs=19&l=en&s=dhs&~tab=bundlestab (visited Jan 12, 2008).

31 This calculation assumes that the printed collection of the Library of Congress, if converted into digital form, would occupy ten terabytes (that is, 10,000 gigabytes). See Lyman and Varian, *How Much Information?* at 3 (cited in note 20).

32 See E. Grochowski and R.D. Halem, *Technological Impact of Magnetic Hard Disk Drives on Storage Systems*, 42 IBM Sys J 338, 340 (2003) (estimating the floor space required to store one terabyte of data over the last several decades).

sion of "higher-end" storage geared toward businesses. The emergence of alternative storage models—and the resurgence of third-party storage services—is itself a signal of the overwhelming amount of commercial data storage at stake.

Any company that stores a substantial amount of data can manage its own servers or outsource that task to a company that specializes in providing secure storage services. As digital technology became more widespread in the 1980s but storage capacity remained costly and bulky, companies outsourced processing and storage tasks to third parties, classified by a 1986 privacy statute[33] as "remote computing services."[34] Third-party storage services are now re-emerging in a somewhat different form, offering internet-accessible services and storing data in server farms located throughout the country.[35] The cost of the server farms necessary to support mass online storage is substantial,[36] but it allows companies to store and manage data more cheaply than they could on their own. Amazon, for example, offers companies such services through its Simple Storage Service ("Amazon S3") at a rate of $0.15 per gigabyte of storage per month.[37]

Online storage services, moreover, will increasingly target consumers as well. In providing its Gmail users free storage space in exchange for the ability to display advertisements, Google is essentially acting as an online storage service as well as a communications pro-

---

33 See Part II for a discussion of this statute.

34 18 USCA § 2711(2) (2007). See Electronic Communications Privacy Act of 1986, S Rep No 99-541, 99th Cong, 2d Sess 10–11 (1986), reprinted in 1986 USCCAN 3564–65 (describing generally the option to process data offsite); Electronic Communications Privacy Act of 1986, HR Rep No 99-647, 99th Cong, 2d Sess 23 (1986).

35 See, for example, Paul Bray, *The Source of Storage Services*, Computer Reseller News UK 25 (May 14, 2007) (describing the growth in online storage and analogizing a corporation keeping its own data to an individual stashing his or her cash under a mattress rather than in a bank); Zach Patton, *Betting the Farm*, Governing 46 (Mar 2007) (discussing the boom of server farms and questioning how much economic benefit they really bring to areas that have offered tax breaks to attract companies building these data storage facilities); Stephanie N. Mehta, *Behold the Server Farm! Glorious Temple of the Information Age*, Fortune 68 (Aug 7, 2006) (describing the rapid construction and operation of server farms to house the data of "Google, Yahoo, MySpace, and other Internet powers"); James Sherwood, *The Online Storage Boom Is on Its Way*, Computer Reseller News UK (Apr 10, 2006) (analyzing the corporate movement to outsource their data management online but warning that steps must be taken to maintain the security of the data).

36 Of particular concern are the energy costs involved both in powering and cooling the servers. As a result, many storage companies have located server farms where electricity is least expensive, such as near the Columbia River in the Pacific Northwest. See Blaine Harden, *Tech Firms Go Mining for Megawatts; Companies Rush to Exploit Region's Cheap Electricity*, Wash Post A3 (July 9, 2006).

37 Thomas Claburn, *Companies Praise Financial Benefits for Amazon's Simple Storage Service*, InfoWeek (July 12, 2006), online at http://www.informationweek.com/story/showArticle.jhtml?articleID=190302909 (visited Jan 12, 2008). See also Amazon S3, online at http://www.amazon.com/gp/browse.html?node=16427261 (visited Jan 12, 2008).

vider. Google offers each user 2.8 GB of free memory; Yahoo recently began offering users of its email service unlimited storage.[38] Despite the costs of the server farms necessary to support this sort of mass online storage, industry participants predict that, on the consumer side, ISPs will eventually offer mass storage as a managed service, in the same way that they now offer internet connectivity.[39] Indeed, in March 2006, Google inadvertently leaked plans to release this sort of functionality—a "GDrive" that would permit users to store files on Google's servers and access them from any internet-enabled device.[40]

In short, although it is difficult to quantify changes in the capacity for digital storage, it is clear that those changes have been dramatic and sustained. For individual consumers, the cost of storage is negligible; for those who are willing to tolerate advertising in the context of email or other applications, storage is essentially free. For businesses, storage costs are much more substantial, but the emergence of a mass online storage industry both lowers those costs and testifies to the overwhelming amount of data involved.

I do not contend that the changing capacity for digital storage itself demonstrates, or accounts for, a shift toward an architecture of perfect memory. The cost of physical storage is simply one cost of retaining data. In the absence of legal restrictions on data retention, and with a permissive legal framework governing transfers of data among private parties, two other costs are relevant here. First, how much data is stored will depend in part on what data is generated in, or capable of being cheaply converted into, a storable form. Second, the costs of storing data include not only the costs of purchasing and maintaining the hardware on which the information will be stored, but also the additional costs of making the data usable through indexing, a search functionality, or both.

In Parts I.B and I.C, I consider the changing architecture of memory in light of the costs of generating, converting, and accessibly maintaining data. For ease of tying the discussion to the discussion of the regulatory framework in Part II, I focus first on the *contents* of com-

---

38 Thomas Claburn, *Yahoo Mail Promises Unlimited Storage*, InfoWeek (Mar 28, 2007), online at http://www.informationweek.com/story/showArticle.jhtml?articleID=198700845 (visited Jan 12, 2008).

39 See Neil McAllister, *Cleversafe Dreams of Distributed Mass Storage Service*, InfoWorld (Jan 8, 2007), online at http://www.infoworld.com/printthis/article/07/01/08/02OPopenent_1.html (visited Jan 12, 2008) (noting that the CEO of Cleversafe declared, "[w]e're having trouble finding ISPs that don't want to offer this kind of service").

40 Verne Kopytoff, *Google's Gaffe Reveals Internal Secrets; Notes Inadvertently Offer a Look at Financial Plans, Future Product*, San Fran Chron C1 (Mar 8, 2006). Google Docs, launched in October 2006, is effectively an online storage service for data in certain formats. See *Google Docs Tour* (2007), online at http://www.google.com/google-d-s/tour1.html (visited Jan 12, 2008).

munications and then on *other data*. With respect to both categories, the general trends are the same: (1) data is being generated in digital form (or easily converted to it); (2) with cost and access issues pulling data to the network "center," even as costs of data storage at network "endpoints" continue to fall; (3) enabling storage of data under a legal regime that imposes minimal (if any) restrictions on data retention.

B. The Generation, Conversion, and Maintenance of Communications Contents

1. Generation of more "storable" data.

The widespread adoption of digital technology generates more communications contents in storable form. In the predigital era, one could certainly retain all of one's written correspondence if physical space constraints permitted. Until recording technology became widely available in the twentieth century, face-to-face communications could be memorialized, if at all, only in an imperfect written form. Similarly, in the past, no copies of telephone calls existed as a matter of routine; those communications could be memorialized only in written form or, once recording technology became widely available, in the unusual case in which a party to the telephone call (or an eavesdropper) actually took steps to record the conversation.

Electronic communications, in contrast, are "born" digital, and thus are immediately stored or storable in compact form. Some copies of electronic communications are retained under the control of the sender or recipient, while other copies are retained by the third party that provides email services to the sender or recipient. The development of digital technology thus dramatically changes the volume of communications that are stored—a category of communications in which perfect storage (at least for some period of time) is the norm displaces or supplements categories of communications involving imperfect or rare storage.

Electronic communications have not entirely supplanted telephone calls, and so the memory of a user's communications is certainly not complete. Yet with the development of Voice over Internet Protocol (VoIP) technology, telephone calls are shifting from a category of rare and technically difficult storage to a category where routine storage is technically feasible. Because VoIP involves the conversion of sound into digital data, followed by its transmission over the internet, telephone calls are technically similar to typical electronic communications, raising the possibility of routine network storage of such calls.[41]

---

[41] See Implementation of the USA PATRIOT ACT: Crime, Terrorism and the Age of Technology, Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of

2. Pulling data to the network center.

Despite the fact that users can cheaply store electronic communications on their own hard drives, accessibility issues increasingly pull communications away from network endpoints into the network center. Service providers, of course, can retain backup copies of subscribers' communications on their own servers to ensure that those communications are properly delivered. There is growing demand, however, for *users* to have greater storage space on the provider's servers so that users can access communications from multiple internet-enabled locations or devices. As noted above, some service providers already provide high-volume storage at little or no cost; others are likely to do so in the near future. The very goal of Gmail and similar services is to entice users to maintain on Google's servers the communications that they might otherwise have maintained on their PCs.

3. Data retention restrictions and incentives.

Finally, the law imposes limited restrictions on the retention of communications contents by service providers. Consider first the communications that a provider retains in backup storage. The federal statute governing the privacy of stored electronic communications, the Stored Communications Act[42] (SCA), imposes no limitations on the provider's practices in this regard. Indeed, the statute even requires storage in some instances, specifically when a governmental entity seeking access to a subscriber's communications includes in its subpoena or court order a requirement that the service provider create a backup copy of the communications sought.[43] Outright restrictions on storage of communications, if any, will necessarily come from the provider's contractual relationship with the subscriber or perhaps from federal and state laws governing unfair trade practices, rather than from direct retention restrictions.

There are, of course, other market forces that constrain a provider. First, a provider may perceive liability and other risks from unauthorized release of a user's communications—risks that counsel in favor of purging backup data. Second, there are some significant limitations on the transfer of communications that may make long-term retention less attractive to the provider itself (as opposed to the sub-

the House Committee on the Judiciary, 109th Cong, 1st Sess 40 (2005) (testimony of Peter P. Swire, Professor of Law, Ohio State University) ("Because VOIP uses the Internet to transmit voice, . . . ordinary users can and will have their phone conversations stored or cached at the Internet network level.").

42 See Electronic Communications Privacy Act of 1986, Title II ("Stored Communications Act"), Pub L No 99-508, 100 Stat 1848, 1860, codified as amended at 18 USCA § 2701 et seq (2007).

43 18 USC § 2704(a)(1) (2000).

scriber) than retention might be in other contexts. In particular, § 2702 of the SCA generally prohibits a provider of an electronic communication service from disclosing the contents of communications without the consent of the originator or intended recipient of the communications.[44]

However these incentives might affect the *provider's* backup practices, the considerations for a *user* are quite different. If the user's communications can remain on the provider's system for a specified period of time or even indefinitely without cost to the user, the user has little incentive to delete them. Moreover, as noted above, providers increasingly compete for subscribers' business by offering greater storage space than the user would have on his or her own hard drive or on other providers' systems. In light of user demand for central storage, companies are likely to perceive that the liability risks of unauthorized access are best addressed through security mechanisms rather than constraints on subscribers' data retention.

C. The Generation, Conversion, and Maintenance of Other Data

1. Generation of more "storable" data.

With respect to other data, I have already alluded to the detailed data trails that result from a user's online browsing, purchasing, and related activities. Some of this data simply did not exist in the predigital world. Physically flipping through the yellow pages generates no storable data; a search for the same information with a search engine will generate information that is both capable of storage and likely to be stored. Physically browsing the books in a bookstore or library generates a data trail only if one is being physically watched; a search for the same books on Amazon will generate a data trail in every case. These phenomena have been extensively considered elsewhere; the point for now is simply that digital technology creates a pool of storable data, some of which could otherwise be collected only by persistent physical observation and some of which would not be available even then.

2. Pulling data to the network center.

In many of the scenarios described above, third parties rather than the data subject will control the data in question. An ISP may

---

[44] See 18 USCA § 2702. A provider can disclose the contents of a communication to a law enforcement agency if the contents were inadvertently obtained and appear to pertain to a crime, or to any governmental entity if the provider believes that a danger of death or serious physical injury requires disclosure without delay. 18 USCA § 2702(b). Although § 2702 makes clear that service providers cannot transfer a subscriber's communications, it contains an important substantive limitation: it applies only to providers of communications services *to the public.* See 18 USCA § 2702(a).

maintain a log of its users' web browsing activities. A website owner can maintain a log of the user's browsing activities on her site, or can provide a link through which a transactional partner (such as an advertising service) will do so.

Two other significant trends in information technology are shifting data from network endpoints to the network center. First, items previously sold as stand-alone "products" are now becoming "services," thereby allowing the collection and generation of information by more third parties. For example, software providers now rarely offer stand-alone software packages for users' PCs; they instead offer something more like a software "service"—a software product that builds in the capability to contact the provider's site for updates, to validate the authenticity of the copy, and so on. These services facilitate the collection of data on usage of the software that was previously unavailable (or confined to just the user's PC). Consider also the difference between a stand-alone VCR and a DVR offered by a cable company or TiVo. The stand-alone VCR generates no data (except that which might be observable by physical surveillance). Because the DVR is linked to a service that provides programming information, it generates data on which programs the user records. Indeed, some DVRs offer central storage rather than storage on a set-top box, an arrangement that necessarily entails the provider's collection of information about which programs the user records. Even with respect to personal computers, software manufacturers are moving toward placing applications themselves on the network rather than at its endpoints. Google Docs is an early example of such a web-based application (and one whose use requires that a user shift her documents to third-party storage with Google).[45] In short, as the product-becomes-service trend continues to develop, the personal computer will become less a collection of stand-alone software and more of a point of access for multiple services.

This product-becomes-service model is closely tied to a second trend in digital technology also involving a move away from the stand-alone personal computer: the trend toward "ubiquitous" or "pervasive" computing.[46] Under a ubiquitous computing model, everyday objects, such as appliances, clothing, and food packages will be em-

45 See *Google Docs Tour* (cited in note 40).

46 See, for example, Jerry Kang and Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 Wash & Lee L Rev 93, 94 (2005) (forecasting that pervasive computing will spread and make "the line between cyberspace and real space … impossible" to identify); Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 Miss L J 1, 3 (2005) (attempting to resolve whether the Fourth Amendment's privacy guarantees may be adapted to a "world of ubiquitous technology").

bedded with wireless computing technology. That technology will allow the routine tracking of minute details about our lives. A refrigerator might issue a warning if food has passed a spoilage date; while at the grocery store, with the aid of a PDA, I might be able to check how many sticks of butter remain in my refrigerator at home. My washing machine might alert me or adjust its settings if I mistakenly include dark clothes in a load of white laundry.

Although such technology is still developing, it is clear that the trend toward pervasive computing will produce a vast amount of data that is capable of being stored, much of which could only otherwise be gathered by physical observation. It remains to be seen whether that data will remain in the hands of the data subject—that is, the technology user—or whether it will be dispersed among third parties. Some ubiquitous computing enthusiasts envision the use of technology to create a unified, autobiographical "lifelog"—an archive that indiscriminately records all personal activities and events.[47] Such an archive, even if controlled and maintained by the technology user rather than single or multiple third-party data holders, would significantly transform the idea of memory as we know it.[48] If the product-becomes-service model continues to prevail, the trend toward ubiquitous computing may produce more data at the network center rather than the network "endpoints." Moreover, to some extent, the convenience that ubiquitous computing promises requires maintaining data in a third party's hands.

3. Data retention restrictions and incentives.

As in the case of communication contents, outright restrictions on the retention of other data generally flow from contractual privacy arrangements or protections against unfair trade practices, not from statutes specifically covering information privacy. There are sector-specific exceptions, but those statutes require destruction of data only when the data is no longer "necessary," and they leave the question of

---

47 See, for example, Alec Wilkinson, *Remember This? A Project to Record Everything We Do in Life*, New Yorker 38 (May 28, 2007) (describing Gordon Bell's project to digitize all aspects of his life); Rachel Ross, *Lifelog: A Useful, Brutal Reality Check; Logged on for Life*, Toronto Star D01 (Sep 8, 2003) (questioning the virtues of digitally recording all aspects of an individual's life, as in Gordon Bell's project).

48 See Martin Dodge and Rob Kitchin, *The Ethics of Forgetting in an Age of Pervasive Computing* 11 (CASA Working Paper Series No 92, 2005), online at http://www.casa.ucl.ac.uk/working_papers/paper92.pdf (visited Jan 12, 2008) (arguing that "life-logs . . . have significant implications to the recording of the present and thus how the past is recalled as opposed to remembered").

necessity entirely within the data collector's discretion.[49] Perceived liability and other risks of data breaches may counsel in favor of purging data; on the other hand, the fact that private parties can with few limitations transfer data to other private parties makes data retention a potentially profitable activity. There are several sector-specific privacy statutes governing the transfer of data, including the Right to Financial Privacy Act[50] (RFPA) (regulating disclosure of financial records), the Fair Credit Reporting Act[51] (FCRA) (regulating disclosure of identifying information and credit reports), the Cable Communications Privacy Act[52] (regulating disclosure of cable viewing activities), the Video Privacy Protection Act of 1988[53] (regulating disclosure of video rental and sales records), and the Health Insurance Portability and Accountability Act[54] and its implementing rules (regulating disclosure of protected health information). To the extent that explicit disclosure limitations are the exception rather than the rule, however, the law provides incentives for companies to retain data in anticipation of future transactions that may be beneficial.

D. Conclusion

This Part has highlighted some of the shifts in the architecture of memory. The shift to digital technology has not only enabled cheap storage of information but has also generated more information that is "born" digital or capable of being made so, including information that was previously unavailable or nonexistent. With respect to communications contents, indefinite storage is attractive to subscribers even if it raises security concerns for service providers. With respect to the range of other data generated through digital transactions—including data that previously could not be routinely captured—current law provides at least some incentives for indefinite data retention by only loosely regulating transactions in data. As the product-

---

49 There are sector-specific exceptions. The Cable Communications Privacy Act, for example, requires providers to "destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected." 47 USC § 551(e) (2000 & Supp 2004). Similarly, the Video Privacy Protection Act requires destruction of personally identifiable information "as soon as practicable, but no later than one year from the date the information is no longer necessary." 18 USC § 2710(e) (2000).

50 Right to Financial Privacy Act of 1978 § 1103, Pub L No 95-360, 92 Stat 3697, codified at 12 USC § 3403 (2000).

51 Pub L No 91-508, 84 Stat 1128, codified in relevant part at 15 USCA § 1681b (2007).

52 Cable Communications Policy Act of 1984 § 631, Pub L No 98-549, 98 Stat 2794–95, codified at 47 USC § 551 (2000 & Supp 2001).

53 Pub L No 100-618, 102 Stat 3195, codified at 18 USC § 2710 (2000).

54 Health Insurance Portability and Accountability Act of 1996 (HIPAA) § 262, Pub L No 104-191, 110 Stat 1936, 2021–31, codified at 42 USC § 1320d et seq (2000 & Supp 2001). See also 45 CFR § 160, 162, 164 ("HIPAA Privacy Rule").

becomes-service model and the pervasive computing model take hold, an architecture of data loss gives way to a developing architecture of perfect memory—where much memory is under the control of third parties rather than the data subject.

II. THE MEMORY GAP AND PRIVATE/GOVERNMENT INFORMATION FLOWS

For government surveillance activities, the legal consequences of the memory shifts described in Part I are quite significant. The increasingly complete architecture of memory preserves more information for government agents to draw from. Much of the data could not have been gathered in the predigital era without substantial and costly forms of physical observation, and in any event would have been costly to memorialize. Moreover, as discussed below, the fact that such information is largely held by third parties makes that information accessible under weaker legal standards. Our "direct" surveillance regimes—regulating government agents' use of surveillance devices and other techniques to capture communications and data or otherwise to observe a target's private activities—are highly protective of privacy. Our "indirect" surveillance regimes, for the most part, are not. I explore these regimes in the pages that follow, focusing first on communications contents, second on communications attributes, and finally on other data.

A. Contents of Communications

1. The "direct" surveillance regime.

Federal law imposes both constitutional and statutory constraints on the direct collection of the contents of communications by government agents. The Supreme Court concluded in *Katz* that eavesdropping constitutes a "search" for purposes of the Fourth Amendment.[55] In the wake of *Katz*, which itself followed a detailed discussion of the requirements for lawful surveillance in *Berger v New York*,[56] Congress adopted Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[57] Also known as the Wiretap Act, the statute requires federal and state officials seeking to "intercept" the contents of a communication to comply with strict requirements, some of which

55 389 US at 353.

56 388 US 41, 53–60 (1967) (invalidating a New York statute that permitted eavesdropping without a showing of probable cause).

57 Pub L No 90-351, 82 Stat 211, codified as amended at 18 USCA § 2510 et seq (2007).

exceed those of typical warrants.[58] Courts have fairly consistently interpreted Title III's definition of "intercept," the key determinant of the statute's scope, to cover only the prospective acquisition of communications as they occur, not the retrospective acquisition of a collection of stored communications.[59] Although the statute initially applied only to wire communications (that is, communications containing the human voice and carried over a telecommunications system) and oral communications (that is, spoken communications in which one has an expectation of privacy), Congress extended the statute in 1986 to cover electronic communications.[60] Law enforcement agents thus cannot acquire the contents of electronic communications in real time without complying with the statute's requirements. The Foreign Intelligence Surveillance Act[61] (FISA), which governs surveillance in the United States (or connected to a United States person) that is designed to acquire the communications of a "foreign power" or an "agent of a foreign power," similarly prohibits the acquisition of communications without the approval of a special court, the Foreign Intelligence Surveillance Court (FISC).[62] Although FISA does not track Title III, it establishes fairly elaborate procedures for agents to gain approval of surveillance activities, including generally requiring a showing of probable cause that the targeted facilities are being used or are about to be used by a foreign power or the agent of a foreign power.[63]

The framework governing agents' acquisition of communications through activities other than "interception" is somewhat different. The Fourth Amendment of course provides strong protection of communications that a user might store on her own computer: if the user has a reasonable expectation of privacy in the contents of the computer, government officials cannot view its contents without obtaining a warrant or meeting one of the relevant exceptions to the Fourth Amendment's warrant requirement. Disputes in such cases often involve chal-

---

58 See 18 USC § 2518 (2000) (describing the procedures required to submit an application for an order to authorize interception). See also Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw U L Rev 607, 630–31 (2003) (characterizing Title III orders as "super-warrants").

59 See, for example, *Fraser v Nationwide Mutual Insurance Co*, 352 F3d 107, 113–14 (3d Cir 2003) (holding that an "intercept" must occur contemporaneously with transmission and does not apply to recovery of stored email); *Steve Jackson Games, Inc v United States Secret Service*, 36 F3d 457, 461–62 (5th Cir 1994) (same); *Wesley College v Pitts*, 974 F Supp 375, 388 (D Del 1997) (same). I discuss the complexities of this issue elsewhere. See Bellia, 72 Geo Wash L Rev at 1391–95 (cited in note 9) (discussing intercepts under Title III and its amendments in 1986 and 2001).

60 Electronic Communications Privacy Act of 1986 (ECPA), §§ 101–11, Pub L No 99-508, 100 Stat 1848, 1848–59, codified as amended in various sections of 18 USCA (2007).

61 Pub L No 95-511, 92 Stat 1783, codified as amended at 50 USCA § 1801 et seq (2007).

62 Id.

63 See 50 USC § 1805(a)(3)(B) (2000).

lenges to warrantless searches and raise questions about whether government agents should have used a warrant—for example, whether the user has consented; whether the user has a reasonable expectation of privacy in a shared computer; and whether someone else has actual or apparent authority to consent to the search.[64]

What about actions of the government that do not involve "interception" in a technical sense, but that involve agents' direct acquisition of communications held by a service provider? For example, suppose government agents seek stored communications from a subscriber's Gmail account. Even if seeking stored communications would not constitute an "interception" for purposes of Title III, another federal statute regulates the acquisition of stored communications. In 1986, Congress passed the Electronic Communications Privacy Act[65] (ECPA), which sought to update federal law to protect emerging communications technologies. A portion of that statute, also known as the Stored Communications Act, regulates access to stored communications and records. The statute prohibits any person from accessing the facility of a communications service provider, or exceeding access to that facility, and thereby "obtain[ing], alter[ing], or prevent[ing] authorized access to" a communication in electronic storage.[66] The statute thus prohibits the direct acquisition of communications from electronic storage within the service provider's system. At the same time, the SCA exempts law enforcement conduct undertaken under Title III or under the SCA's own government access provisions, discussed below.[67] The latter provisions deal only with *compelled production* of communications from a service provider,[68] not with direct acquisition of communications from a service provider's system. In practice, then, the only means for law enforcement agents to acquire stored communications directly, without simply compelling the service provider to disclose them, is in compliance with the procedures of Title III.

In sum, the regime for direct acquisition of contents of communications is quite robust: for ongoing acquisition of communications, it requires Title III's super-warrant procedure or compliance with FISA; for acquisition of communications stored on a user's own computer, it requires a warrant or an exception to the warrant requirement. When

64 See, for example, *United States v Morgan*, 435 F3d 660, 663–64 (6th Cir 2006) (analyzing the consent and apparent authority questions); *United States v Grimes*, 244 F3d 375, 383 (5th Cir 2001) (discussing the reasonable expectation of privacy question).

65 ECPA §§ 101–11, 100 Stat at 1848.

66 18 USC § 2701(a) (2000).

67 See 18 USC § 2701(c)(3) (2000) (exempting from § 2701(a) liability those individuals whose activities are authorized under §§ 2703, 2704, or 2518).

68 See 18 USCA § 2703.

communications are stored by a third-party service provider, the only "direct" acquisition the SCA contemplates is through compliance with the procedures of Title III.

2. The "indirect" surveillance regime.

When service providers retain copies of communications on their systems and government agents seek to acquire them from the service provider rather than to acquire them directly, the legal framework is far more uncertain. In *Miller*, the Supreme Court held that the target of an investigation has no reasonable expectation of privacy in information he voluntarily discloses to a third party, even if he discloses the information for a limited purpose and with the expectation that the third party will not betray his confidence.[69] The legal framework governing agents' efforts to acquire communications from service providers thus depends upon whether the logic of *Miller* extends to communications stored with a service provider—a question that the courts have not yet answered definitively.

In July 2006, the district court in *Warshak v United States*[70] became the first Article III court to squarely address what legal process government agents must use to compel production of communications from a third-party service provider.[71] In *Warshak*, the target of a fraud investigation challenged the government's use of a subpoena-like process to compel service providers to produce thousands of emails stored on their servers, including draft emails, sent emails, and emails the target had already viewed.[72]

Among the government's arguments in defending the agents' approach was the claim that an email subscriber cannot have an expectation of privacy in communications stored with a provider because such communications are "disclosed" to the provider in the *Miller* sense.[73] This position did not carry the day in the district court or the United

69 425 US at 443.

70 2006 US Dist LEXIS 50076 (SD Ohio), affirmed 490 F3d 455 (6th Cir 2007), vacated for rehearing en banc 2007 US App LEXIS 23741 (6th Cir 2007).

71 2006 US Dist LEXIS 50076 at *8–20. Along with Professor Susan Freiwald of the University of San Francisco School of Law, I submitted an amicus brief supporting Warshak before the Sixth Circuit panel, on behalf of professors of internet law and electronic privacy law.

72 Id at *2–3.

73 See United States of America's Memorandum in Opposition to Plaintiff's Motion for Temporary Restraining Order and/or Preliminary Injunction, Case No 1:06-cv-00357-SJD, 7–9 (SD Ohio filed July 15, 2006); Brief of the United States of America, *Warshak v United States*, Civil Action No 06-4092, 36–40, 43–45 (6th Cir filed Oct 11, 2006), online at http://www.cdt.org/security/20061127warshak.pdf (visited Jan 12, 2008).

States Court of Appeals for the Sixth Circuit,[74] which both held that use of a subpoena-like process to compel disclosure of a subscriber's email, without prior notice to the subscriber, violates the Fourth Amendment. The government, however, pressed the *Miller* analogy in its request for en banc review in the Sixth Circuit,[75] which the court recently granted. This understanding of *Miller*'s applicability has long guided the Justice Department's interpretation of provisions of the SCA governing compelled production of communications. In particular, the SCA distinguishes between two categories of communications—those in "electronic storage" and those that are not—and explicitly provides warrant-level protection only for those that are in electronic storage. The Justice Department has argued that courts should give weight to Congress's apparent determination that not all electronic communications are subject to a warrant requirement.

Federal law defines "electronic storage" as any temporary storage of a communication "incidental to the electronic transmission" and any storage of a communication "by an electronic communication service for purposes of backup protection."[76] The Justice Department has historically interpreted this definition quite narrowly, to apply to emails stored temporarily on a service provider's system prior to being retrieved by a subscriber.[77] The emails retrieved in the *Warshak* case—that is, emails that Warshak had already viewed as well as those that Warshak himself sent—are outside of electronic storage as the DOJ interprets the term. That interpretation necessarily rests on the premise that compelling production of such emails without a warrant raises no Fourth Amendment problems—a premise that, in turn, rests on applicability of the *Miller* line of cases in this context.

This longstanding interpretation of the scope and structure of the SCA has not gone unchallenged, even before the *Warshak* decision.

---

74 See *Warshak v United States*, 490 F3d 455, 475 (6th Cir 2007) (holding that "[w]here the third party is not expected to access the e-mails in the normal course of business, however, the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement").

75 The government's en banc petition mainly addressed procedural issues, but it included criticism of the court's approach to the underlying Fourth Amendment issue. Petition of the United States for Rehearing en Banc, *Warshak v United States*, Civil Action No 06-4092, 13 (6th Cir filed Aug 1, 2007), online at http://volokh.com/files/Warshak_en_banc_petition.pdf (visited Jan 12, 2008) (citing *Miller* and arguing that the constitutionality of compelled disclosure of electronic communications depends "not on the Fourth Amendment's specific requirements for warrants, but on reasonableness under the circumstances"). Because the en banc court's action vacates the panel decision, the government is likely to continue to press the *Miller* analogy on rehearing en banc.

76 18 USC § 2510(17) (2000 & Supp 2001).

77 See DOJ, *Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations* § III.B (2002), online at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (visited Jan 12, 2008).

Because the SCA protects communications held in electronic storage with a provider against unauthorized acquisition by private parties and government agents alike, a number of cases construing key statutory terms have involved disputes between private parties. In such cases, courts have divided on how to construe the term "electronic storage." While several courts have concluded that the term covers only those communications temporarily stored prior to retrieval by a subscriber,[78] one court has suggested,[79] and another has held[80] that the backup protection prong of the definition is sufficiently broad to encompass copies of communications that a subscriber chooses to leave on a provider's server after downloading them. In disputes between private parties, of course, the choice between these two interpretations of the term "electronic storage" does not implicate the Fourth Amendment. Put another way, courts construing the relevant terms in cases involving private parties have not had an opportunity to consider how concerns about avoiding constitutional questions might cabin interpretation of the statutory language. The legislative history of the SCA itself suggests conflicting views on how the Fourth Amendment protects electronic communications.[81]

In *Warshak*, neither the district court nor the court of appeals directly considered the scope of the term "electronic storage," but the decisions make clear that the DOJ's narrow interpretation of electronic storage would render the SCA unconstitutional in at least some circumstances. At the same time, however, the *Warshak* courts' endorsement of a warrant requirement for indirect communications surveillance was not complete. Both courts seemed to take the view that a subpoena-like process would satisfy the Fourth Amendment so long as the government gave the subscriber prior notice of the acquisition. Moreover, it is unclear whether the courts' approach will survive en banc review in the Sixth Circuit.

In sum, the shifting architecture of memory has significant consequences for rules governing agents' access to communications. As communications contents are increasingly held by service providers,

---

78 See, for example, *In re DoubleClick Inc Privacy Litigation*, 154 F Supp 2d 497, 512 (SDNY 2001); *Fraser v Nationwide Mutual Insurance Co*, 135 F Supp 2d 623, 636 (ED Pa 2001).

79 *Fraser*, 352 F3d at 114 (noting that "it seems questionable that the transmissions were not in backup storage" after emails had been viewed but not yet deleted by a user).

80 *Theofel v Farey-Jones*, 359 F3d 1066, 1075–77 (9th Cir 2004).

81 Compare S Rep No 99-541 at 3 (cited in note 34) (expressing fear that communications in the hands of service providers "may be subject to no constitutional privacy protection"), with HR Rep No 99-647 at 22 (cited in note 34) ("It appears likely . . . that the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required."), 23 (suggesting that the contents of some electronic communications in storage enjoy a higher degree of Fourth Amendment protection than customer records).

they are removed from the robust restrictions on direct government access drawn from the Fourth Amendment, from Title III, and from FISA. Once held by third parties, communications are in a zone of uncertainty with respect to the Fourth Amendment. The SCA does contain a warrant requirement, but it is unclear whether that requirement reaches only those communications not yet delivered to a recipient or if it also reaches communications delivered to a recipient but maintained on the server. The *Warshak* decision would have simplified matters by requiring a warrant even as to communications held by a service provider and already retrieved by the subscriber. But much uncertainty remains about the scope of that decision and whether it will withstand further review.

B. Communication Attributes

I now turn to communication "attributes," a term I use to describe data about communications, such as information about the origin, destination, and duration of communications.[82] Although the direct surveillance regime governing "direct" acquisition of communications attributes is far less protective than that for direct acquisition of communications contents, the indirect surveillance regime in some respects provides still less protection.

1. The "direct" surveillance regime.

The law treats communications attributes quite differently from the contents of communications. In terms of the Fourth Amendment, the key precedent is the 1979 case of *Smith v Maryland*.[83] There, the Supreme Court held, following *Miller*, that the user of a telephone has no expectation of privacy in the number he dials because he voluntarily conveys that number to the telephone company so that the call can be connected.[84] *Smith* involved the use of a pen register—a device that records the number of an outgoing call—but its principles apply equally to the use of a trap and trace device to capture the number of an incoming call. In 1986, in response to *Smith* and as part of the Electronic Communications Privacy Act, Congress adopted some restrictions on the use of pen registers and trap and trace devices.[85]

---

82 See Susan Freiwald, *Uncertain Privacy: Communication Attributes after the Digital Telephony Act*, 69 S Cal L Rev 949, 953 (1996).

83 442 US 735 (1979).

84 Id at 744–45.

85 Electronic Communications Privacy Act of 1986, Title III ("Pen Register Act"), Pub L No 99-508, 100 Stat 1848, 1868, codified as amended at 18 USC § 3121–27 (2000 & Supp 2002).

Although the statute requires government agents to seek a court order before using a pen register or trap and trace device, the standard on which an order will be granted is far lower than that required for a warrant. In particular, the statute states that a judge "shall" enter an order authorizing use of the device if an attorney for the government certifies that use of the device will yield information "relevant" to an ongoing criminal investigation.[86] As amended by the Patriot Act,[87] these provisions cover not only dialing information associated with telephone calls, but also addressing, signaling, and routing information associated with wire and electronic communications. FISA imposes similar constraints on the gathering of addressing, signaling, and routing information for foreign intelligence purposes. Rather than certifying to a judge that the use of the device will yield information relevant to an ongoing criminal investigation, an attorney for the government must certify that use of the pen register and trap and trace device will yield information that is relevant to an ongoing foreign intelligence or international terrorism investigation.[88]

Finally, in a discussion of communications attributes, it is worth noting the slightly different rules governing acquisition of location information that can be derived from use of cell phones. By "triangulating" data from cell phone providers concerning the cell towers "hit" by a targeted cell phone, government agents can approximate the location of the phone. The Communications Assistance for Law Enforcement Act[89] (CALEA) bars officials from relying solely on the pen register and trap and trace statute to obtain this sort of location information. When seeking to triangulate cell phone data in real time, then, law enforcement officials initially relied on a "hybrid" approach that invoked two sets of statutory provisions. In particular, they sought to rely on the pen/trap provisions as well as provisions in the SCA allowing law enforcement officers to compel production of certain records concerning customers of communications service providers.[90] The SCA allows law enforcement officials to compel production of customer records without a warrant. In claiming that a hybrid pen/trap and SCA order was sufficient to permit law enforcement agents to triangulate cell data, the government argued that: (1) the location information was "signaling" information as defined by the pen register

86 18 USC § 3123(a).

87 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"), Pub L No 107-56, 115 Stat 272 (2001).

88 50 USCA § 1842(c)(2) (2007).

89 Communications Assistance for Law Enforcement Act § 103(a), Pub L No 103-404, 108 Stat 4279, 4280–81, codified at 47 USC § 1002(a) (2000).

90 18 USCA § 2703(c).

and trap and trace statute; (2) CALEA merely said that that statute could not be the *sole* basis for gathering that information, not that it would not be sufficient if supplemented by other relevant authority; and (3) that an order satisfying the predicates of both the pen/trap statute and the customer records provisions of the SCA would be sufficient.[91] Initially, numerous magistrate judges accepted the government's argument and granted the requested "hybrid" order. After two magistrate judges held (based on interpretation of the relevant statutes) that the government could not obtain the information without a warrant supported by probable cause,[92] several others followed in rejecting the government's "hybrid" authority theory.[93] Accordingly, as a matter of statutory interpretation, several courts have treated the acquisition of location information yielded by triangulation of cell phone data as requiring a warrant.

In sum, although the direct surveillance regime is less protective of communications attributes than of communications contents, federal statutes require a court order issued on a relevance standard for acquisition of such attributes. For location information concerning mobile devices, courts have as a matter of statutory interpretation required a warrant.

2. The "indirect" surveillance regime.

Just as Title III applies only to contemporaneous acquisition of communications, the criminal and foreign intelligence pen register and trap and trace provisions have been understood to apply only to the prospective acquisition of communications attributes. When such data is stored, a different framework applies. In particular, as noted above, the SCA contains provisions governing the retrospective acquisition

---

91 See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F Supp 2d 747, 761 (SD Tex 2005); *In the Matter of an Application of the United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F Supp 2d 294, 316 (EDNY 2005).

92 See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F Supp 2d at 765; *In the Matter of an Application of the United States for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F Supp 2d at 324.

93 See, for example, *In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F Supp 2d 947, 957–58 (ED Wis 2006); *In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information*, 407 F Supp 2d 134, 135 (DDC 2006); *In re Application of the U.S. for an Order Authorizing Installation and Use of Pen Register*, 415 F Supp 2d 211, 219 (WDNY 2006); *In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [sealed] and [sealed] and the Production of Real Time Cell Site Information*, 402 F Supp 2d 597, 600 (D Md 2005).

of stored customer records from service providers;[94] these records can contain precisely the same information that prospective use of pen registers and trap and trace devices yield. Although the SCA's standards are similar to those in the pen/trap statute, other authorities permit production of information on lower standards. Moreover, when law enforcement officials use a pen register or trap and trace device to capture attributes of ongoing communications, they will have available to them only the data on communications occurring at a particular moment in time. If such data is then stored and retained indefinitely, law enforcement officials can draw data from that vast pool indefinitely.

The SCA creates two classes of customer data. Where government agents seek basic subscriber records, such as the subscriber's name, address, records of call connections or the time and duration of sessions, and any number or temporarily assigned network addresses for the communications, the statute requires only that the agents present the provider with a grand jury or administrative subpoena.[95] For customer records beyond these basic records, the statute requires, at a minimum, a special court order under § 2703(d), issued based on a showing of "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought are relevant and material to an ongoing criminal investigation.[96] The showing required under § 2703(d) is thus roughly equivalent to that required under the pen/trap statute, except that the government must demonstrate relevance rather than merely certifying it.

On the foreign intelligence side, however, the indirect surveillance alternatives are more permissive. In particular, § 2709 of the SCA grants FBI investigators the authority in certain foreign intelligence investigations to issue so-called "national security letters" (NSLs) to compel the production of records concerning wire and electronic communications, described in the statute as "toll billing records information" and "electronic communication transactional records."[97] Although the initial version of this provision required the FBI to certify that the records sought were connected to a foreign intelligence investigation and that there were specific and articulable facts linking the information sought to a foreign power or agent of a foreign power under FISA,[98] the Patriot Act removed the latter requirement.[99] Thus, the FBI can request stored records of noncontent communications

94 18 USCA § 2703(c).

95 18 USC § 2703(c)(2) (2000 & Supp 2001).

96 18 USCA § 2703(c)(1); 18 USC § 2703(d) (2000 & Supp 2001).

97 18 USCA § 2709.

98 18 USC § 2709 (2000).

99 Patriot Act § 505, 115 Stat at 365, codified at 18 USC § 2709(b) (2000 & Supp 2001).

attributes merely upon a showing of relevance to a foreign counterintelligence investigation and without that showing ever having been made to a court.

In sum, the shifting architecture of memory for communications attributes will have important consequences for government access rules. Government agents' direct acquisition of some communications attributes is governed by the pen register and trap and trace statute added as part of ECPA in 1986, whereas its indirect acquisition is governed by the SCA. The similar legal standards might make that shift seem insignificant, but those similar standards apply to vastly different quantities of data. The pen/trap statute is self-limiting because it only applies to ongoing communications. The SCA provision, in contrast, can allow agents to collect historical data that would have been virtually impossible to collect in real time. In other words, the low cost and high density of current storage technologies make indefinite retention of data possible, thus preserving a store of information for government access for much longer periods of time than the information would ordinarily be available for direct observation.

C. Transactional and Passive Data

Finally, I consider the direct and indirect surveillance regimes governing a residual category of data that does not fall into the communications contents or communications attributes categories. Some of the data might be considered "transactional" data analogous to the business records at issue in *Miller*, insofar as it is provided in order to consummate a transaction. Such data can include information arising from particular transactions or interactions with third parties, such as banks, credit card companies, and websites. I also have in mind, however, the sort of "passive" environmental or experiential data that a pervasive computing environment is likely to produce.

1. The "direct" surveillance regime.

The direct surveillance regime with respect to the gathering of noncommunications data is that imposed by the Fourth Amendment and any relevant statutes exceeding Fourth Amendment requirements. That is, where gathering particular information would invade a reasonable expectation of privacy, the Fourth Amendment would require a warrant. Importantly, when government agents gather the information directly rather than from a third party who is also privy to it, the mere fact of third-party involvement does not defeat an expectation of privacy. For example, if law enforcement officials intercepted a communication from a bank customer to the bank directing a transfer of certain funds, current doctrine would insist that the interception be

governed by protective direct surveillance rules rather then less stringent indirect surveillance rules. Put another way, the mere involvement of a third party does not eliminate a target's expectation of privacy; the fact that the third party *could* reveal the details does not relieve government agents of the obligation to comply with the Fourth Amendment's warrant requirement when government agents seek the information directly.

Similarly, the sorts of passive information that pervasive computing will yield, if directly observed, would in many cases require compliance with the Fourth Amendment's warrant requirement. *Kyllo* itself provides one example, for it suggests that activity to detect information about environmental variables inside a home—in that case, the heat emanating from the home—requires a warrant.[100] That is, if a surveillance-enhancing device yields the same information that previously would have required physical entry into the home, the Fourth Amendment requires the agents to proceed as if they were physically entering it.

2. The "indirect" surveillance regime.

Although *Miller*'s implications for communications held by service providers are unclear, its implications for other transactional partners are fairly straightforward. When one transmits information to a third party for the purpose of processing a particular transaction and for which the content of the information is relevant, courts will treat the information as having been "disclosed" and thus not subject to a reasonable expectation of privacy. In some cases, the involvement of multiple transactional partners—a retailer or intermediaries such as service providers, credit card companies, and so on—will allow the same transactional information to be available from multiple third parties.

With respect to the passive environmental or experiential data produced by developments in pervasive computing, application of *Miller* is somewhat more complicated. No deliberate "transmission" of information occurs; the information is simply "exposed" to third parties by virtue of the pervasive computing application involved. An early example of such technology might be the increasingly sophisticated digital meters that are being designed to measure electricity usage at frequent intervals and transmit that information wirelessly to a utility company.[101] These "demand response" systems produce finely grained information that could ordinarily be collected only by direct

100 See 533 US at 40.

101 See Matt Richtel, *Conservation at the Touch of a Button*, NY Times H9 (Nov 7, 2007), online at http://www.nytimes.com/2007/11/07/business/businessspecial3/07cutoff.html (visited Jan 12, 2008).

surveillance. Once that information is "exposed" to the utility company, however, its compelled production, if analogized to the compelled production of transactional information in *Miller*, would not require a warrant.

Several sector-specific privacy statutes do govern the disclosure of certain types of records to the government. For example, the Right to Financial Privacy Act[102] forbids a financial institution from disclosing a customer's financial records,[103] while the Fair Credit Reporting Act[104] prohibits credit reporting agencies from disclosing credit reports (beyond certain identifying information).[105] Other sector-specific statutes and regulations prohibit cable providers from disclosing cable records[106] and prohibit videotape service providers from disclosing video rental records.[107] These same statutes permit compelled disclosure of these records, with varying standards. The most protective statute is the Cable Communications Privacy Act. To obtain a court order compelling disclosure of records under the act, a government entity must demonstrate "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case."[108] Other statutes are far less protective. The RFPA, for example, authorizes use of administrative and grand jury subpoenas to compel disclosure of records, as long as the subject of the data has the opportunity to contest the subpoena.[109]

These sector-specific rules ultimately create only a patchwork of protection for transactional data. Because *Miller* may apply in a variety of contexts in which a person generates data that is later held by a third party, the statutes requiring a warrant in this situation form the exception rather than a rule: outside of these contexts (and in the absence of contractual restrictions or restrictions deriving from prohibitions on unfair trade practices), government entities can compel a third party to produce records with a grand jury or administrative subpoena without prior notice to the subject of the data. In addition, because the statutes focus on the activities of particular classes of record holders rather than the records themselves, they do not fully protect even those records they cover. For example, the RFPA protects

---

102 Right to Financial Privacy Act § 1103, 92 Stat at 3697, codified at 12 USC § 3403 (2000).

103 See 12 USC § 3403(a).

104 84 Stat at 1128, codified in relevant part at 15 USCA § 1681b (2007).

105 See 15 USC § 1681f (2000).

106 See 47 USC § 551(h).

107 See 18 USC § 2710.

108 See 47 USC § 551(h)(1).

109 12 USC §§ 3402, 3405, 3407 (2000). The Act also authorizes the use of search warrants to compel disclosure of records without prior notice to the data subject. 12 USC § 3406 (2000).

against a financial institution's disclosure of financial records, but not against the disclosure of financial records by another third party who might lawfully have acquired such records. Finally, even the statutes providing warrant-like protection contain important exceptions, particularly in the case of national security investigations. The FCRA and the RFPA, for example, both allow certain agencies to compel disclosure of records by issuing national security letters analogous to those discussed with respect to communications attributes.[110] Although each specific NSL authority differs, all NSL provisions allow officials in the executive branch to compel disclosure of material upon certification of relevance to a national security investigation.

III. CLOSING THE LAW'S MEMORY GAP

The discussion in Part II suggests that the changing architecture of memory—its increasing scope, and the fact that much of it is in third-party control—has destabilizing effects on our communications surveillance law regime. Communications that could once be acquired only prospectively, at a specific moment in time, and under strict standards, can now be acquired retrospectively, at any moment in time, and under less stringent standards. Communications attributes that could once be acquired prospectively and at a specific moment in time (under an admittedly less stringent standard) can now be acquired retrospectively, at any time, from a far broader pool of information than direct acquisition could have produced. Finally, the categories of transactional data available from third parties are expanding dramatically and are available indefinitely.

How should we evaluate these trends, and how, if at all, should the law respond to them? I do not claim that the law can or must require data destruction across the various categories of information discussed here, although there may be good reasons for companies, particularly those holding transactional data, to anonymize or destroy data after a certain time period. I also do not address the consequences of data transfers from one private party to another, though the consequences for such practices of the changing architecture of memory may be quite significant. I argue that with respect to some categories of information, we must harmonize the direct and indirect government surveillance regimes, and harmonize them in the direction of the more protective direct surveillance regimes. My analysis proceeds in three steps. I first consider in Part III.A whether developments in technology or other market changes are likely to restore

110 See 12 USCA § 3414(a)(5)(A) (2007); 15 USCA § 1681u(a)–(c) (2007).

communications and other information to legal categories subject to more direct and thus more highly protected surveillance. In other words, I consider the possibility that even if current shifts raise significant information privacy concerns, those shifts are likely to reestablish an equilibrium in which information returns to more protected categories.

I then confront these privacy concerns more directly in Part III.B. One could argue that whatever level of information privacy may have resulted from the combination of the prevailing legal regime and the imperfect architecture of memory, there is no reason for the law to privilege surveillance imperfections. Evaluation of that argument to some extent requires delving into normative conceptions of information privacy. Such conceptions often do not produce an account of information privacy that is finely grained enough to dictate particular substantive rules or institutional arrangements. I nevertheless argue that whatever level of information privacy such theories might produce as a matter of first principles, there are strong arguments for favoring stable application of certain key constitutional and quasi-constitutional baselines in surveillance law. Although formulated in terms of particular surveillance techniques, those baselines are concerned at their core with the information acquired rather than the techniques themselves. In Part III.C, I suggest how we might translate those baselines for a world of increasingly perfect memory.

A. Technological Change and Other Market Developments

Parts I and II demonstrated that the increasingly perfect architecture of memory has shifted information out of categories involving highly regulated surveillance. These changes are significant, however, only if they reflect a new equilibrium rather than a temporary pendulum swing. We therefore must consider more fully any trends that might cut against data retention. Part I discussed some of these trends, including companies' concerns about the liability and other risks of large-scale data breaches.[111] Those concerns, however, are likely to be more prominent with respect to collection and retention of transactional data than with respect to retention of communications contents. Transactional data is often retained for the benefit of the company rather than for the benefit of the subject of the data, and the company's retention policy is unlikely to be a major marketing tool. For providers that store communications, in contrast, the user's ability to maintain communications indefinitely is itself a selling point—making

111 See Part I.C.3.

it far more likely that the provider will respond to liability concerns by investing in security rather than purging data.

Even for providers that retain transactional data, investing more heavily in security measures and purging data are simply two ways to forestall a large-scale data breach, and the mix a company chooses will take account of the opportunities lost when the company purges data. In other words, it is unlikely that the danger of a *private* party's breach of a company's servers will fully counter the trend toward data retention; more likely, it will cause the company to insure against such a breach or otherwise internalize the costs of securing the network. Moreover, there is little reason for a provider settling upon a data retention policy to factor government access rules into its decisions. Current statutes contemplate government reimbursement for the direct costs a provider incurs for complying with a government request for information.[112] The secrecy that generally surrounds government requests will also make other, indirect costs of compliance—such as the reputational costs a provider may experience by virtue of disclosing information to government agents—less significant, and any such costs may be balanced by the "good citizen" image that the provider's compliance can promote.

Potentially more relevant are mechanisms that may develop to allow users to retain more technical control over their stored communications even while they are maintained on third party servers. Consider a possible model for the remote storage of documents that is somewhat more complex than that prevailing today. Rather than retaining a full file on a particular computer, a provider might distribute pieces of the file across different servers, so that no single server holds all pieces of it. These pieces would be reassembled into the whole file only when the subscriber (or the subscriber's computer) produces a particular security credential.

Even if this remote storage model were to prevail, it is unclear that it would shift communications back from the category of largely unregulated surveillance to the category of highly regulated surveillance. The third party would hold pieces of the file rather than a single file, so in theory it would be more difficult for the government simply to compel the provider to produce the stored file. Although such an approach may have important security benefits (by rendering attacks on the provider's servers relatively less effective), it is unlikely to affect the provider's ability to comply with the government's request for

112 See, for example, 18 USC § 2518(4) ("Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.").

disclosure of communications. Among the forces driving the market toward remote storage, of course, is the ease with which subscribers can access files from multiple computers or devices. Much of the convenience would be lost if the provider did not offer a mechanism for reassembling the file in the event that the security credential were unavailable to a legitimate subscriber. If the provider escrowed or archived the credential, or if government agents could replicate it through a "brute force" attack[113] (as they have successfully done in most cases involving encryption), then the availability of pieces of the file on the provider's servers may be enough to keep such information in the less stringent indirect surveillance regime.

In short, it seems unlikely that developments in technology alone will move communications and data back into the more protective directive surveillance regimes.

B. Normative Conceptions of Information Privacy

Even if the evolving architecture of memory has brought a new equilibrium, it does not follow that we must respond by reviving the old one. There is, after all, nothing inevitable about the sort of surveillance imperfections that the new architecture of memory overcomes. Consider a parallel example from copyright law. Many scholars argue that technology "perfects" a content provider's control over the scholar's work, allowing the content provider to block uses that the copyright law would permit. Scholars who object to this development claim that this "perfection" of control shrinks the space for uses of a work that the law, combined with the copyholder's imperfect technical control, has always permitted. Such views embed normative claims about the value of public uses as well as predictive claims about the amount of control necessary to supply incentives for creation. Those who are less concerned about public uses or make different predictions about how to stimulate development of new works are unlikely to share these concerns about the perfection of a copyright holder's control.

Similarly, evaluating the consequences of the changing architecture of memory to some extent requires us to draw upon normative theories of information privacy. Such theories will obviously call for protection of different underlying interests, for different reasons, with different levels of protection afforded, under different institutional arrangements and procedures. Consider three (overlapping) categories of theories of the value of information privacy: theories focusing

---

[113] A brute force attack involves the use of raw computing power to try every possible key. See, for example, Matt Curtin, *Brute Force: Cracking the Data Encryption Standard* 23 (Copernicus Books 2005).

on the constitutive importance of privacy (that is, the importance of privacy for autonomy and individual self-determination);[114] those focusing on the role of information privacy in ensuring a robust exchange of ideas, either as a good in and of itself or for the contributions of such an exchange to the political process;[115] and those viewing privacy through the lens of economic utility.[116]

These divergent approaches might call for protection of different underlying interests. For example, normative theories of privacy that focus on autonomy and self-determination are more likely to call for protection of a "dignitary" interest in privacy than are theories focusing on economic utility. Ensuring information privacy might instead mean guaranteeing the secrecy of certain information, regardless of the invasion used to acquire it. As many scholars have pointed out, behaviors in commercial transactions tend to demonstrate that consumers neither expect nor are willing to pay to maintain *complete* secrecy of information, but rather may wish to maintain secrecy selectively vis-à-vis certain potential recipients (such as the government). Those who favor constitutive or deliberative approaches to privacy might perceive selective secrecy as necessary to ensuring unfettered communication, whether in the development of individual preferences or for benefits in the political process. Even those who approach information privacy questions from the perspective of economic utility might recognize the costs of a no-privacy condition.

Although different normative conceptions of privacy may point to the need to protect different underlying interests, each conception can coexist with a regime involving some level of government surveillance activity, if only because some level of security is necessary for the individual and collective self-determination that information privacy is thought to support. Put another way, no normative conception

---

114 See, for example, Cohen, 52 Stan L Rev at 1423 (cited in note 17) (advocating "a dynamic theory of informational privacy . . . that focuses on the conditions for meaningful autonomy").

115 See, for example, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand L Rev 1609, 1651 (1999) ("In the absence of strong rules for information privacy, Americans will hesitate to engage in cyberspace activities—including those that are most likely to promote democratic self-rule.").

116 See, for example, George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J Legal Stud 623, 625 (1980) (characterizing privacy as a property right in information and discussing economic consequences of errors in or misuse of this information); Richard A. Posner, *The Right of Privacy*, 12 Ga L Rev 393, 394 (1978) (analyzing privacy as an "intermediate good" and assuming that people do not "desire or value privacy or prying in themselves but to use these goods as inputs into the production of income or some other broad measure of utility or welfare"). But see Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Georgetown L J 2381, 2383 (1996) (arguing that economic analysis of privacy has failed to account for "benefits to privacy beyond the 'taste' for privacy that an individual may have" and has inadequately analyzed default rules for subsequent disclosure of another's personal information).

of privacy entirely excludes the possibility of communications surveillance. One's normative precommitments might call for insistence on a higher substantive standard (probable cause as opposed to relevance) or a particular institutional arrangement (involving judicial rather than executive evaluation of whether probable cause exists), but all would accept the basic goal of a communications surveillance law regime: to establish appropriate standards and institutional arrangements for moderating competing security and privacy interests.

The flip side of this point, which I also take as a given, is that no normative conception of privacy is consistent with a view that security benefits flow inexorably from the gathering of *more* information. That is, the mere fact that more information exists in storable form and is thus indefinitely available for government examination does not itself create the imperative to collect and analyze that information. Other factors—pressing concerns about terrorism, for example—may create imperatives for government entities to use all the information that is accessible to them. If so, the questions shift to what *standards* should govern access to the information, under what *procedures* (*or institutional arrangements*), and, perhaps most critically, *who*—the executive, the legislature, or the courts—gets to select these standards and procedures.

Under current law, the Fourth Amendment's "reasonable expectation of privacy" test of course acts as a trigger for answers to each of these questions. When a court determines that a particular government tactic invades a reasonable expectation of privacy, the court thereby dictates both a standard for access (generally probable cause) and the institutional arrangement (review by a neutral and detached magistrate). When a particular government tactic does not invade a reasonable expectation of privacy, the standards and institutional arrangements are left to the legislature or, in its silence, the executive.

But new technologies in general, and the changing architecture of memory in particular, present two obvious and related challenges for the reasonable expectation of privacy test. The first concerns whether the assessment of whether government action "invades" a reasonable expectation of privacy depends upon the *method of acquiring* data or information or the *type of information or data* that is acquired. The *Katz* Court seemed to focus on the latter, insofar as it suggested that one who occupies a telephone booth "is surely entitled to assume that *the words he utters* into the mouthpiece will not be broadcast to the world" and rejected the argument that government agents' eavesdropping did not implicate the Fourth Amendment because "the *surveillance technique . . . involved no physical penetration* of the tele-

phone booth."[117] Similarly, the Court in *Kyllo* focused heavily on the fact that the *information yielded* by a thermal imaging device was information about what was going on inside of the target's home.[118] At the same time, the *Kyllo* Court suggested that widespread use of a particular surveillance-enhancing device might defeat the reasonableness of an expectation of privacy, suggesting that even the Fourth Amendment's protection of a most sensitive category of information—information on what goes on in the home—may be limited to use of particular surveillance techniques.[119]

This ambiguity about whether the measure of a putative invasion of privacy should depend upon the *means* or the *result* of the invasion complicates legislative efforts to implement the Fourth Amendment. In the case of communications surveillance, Congress has translated rules that seem to focus on the privacy of the information that is acquired into rules that focus on the use of particular techniques or devices. Title III, for example, protects the contents of communications, but only against one form of acquisition—interception—and courts have construed the statute not to apply to use of other means to acquire functionally equivalent communications. Whether this device-based focus results from the courts' interpretation of the reasonable expectation of privacy test or instead reflects a legislative gloss on that test, it has the practical effect of privileging *executive* choices about the standards and procedures under which surveillance activities will proceed. That is, once the *Katz* holding is codified as a rule prohibiting "interception" without a Title III order, that fairly narrow rule permits other surveillance techniques yielding the same information to prevail unless and until Congress or the courts supply an alternative rule. The pre–Patriot Act pen register and trap and trace device statute provides another example of the degree of executive control over the standards and procedures governing surveillance, albeit a statutory rather than constitutional one.[120] Prior to passage of the Patriot Act, the pen/trap statute was written in terms that appeared to relate specifically to devices used to acquire *dialing* information associated with an incoming or outgoing telephone call. The development of electronic communications raised the question whether addressing information—not to mention a range of other information—associated with electronic communications fell under the statute and therefore required

117 389 US at 352 (emphasis added).

118 533 US at 34.

119 Id at 40 (recognizing that defendant's expectation of privacy was reasonable in part because surveillance was conducted with "a device that is not in general public use").

120 See 18 USC §§ 3121–27.

law enforcement compliance with certain procedures.[121] The DOJ took the position that addressing information associated with electronic communications did fall under the statute, but the particular language of the statute would have made it easy for the DOJ to instead conclude that the information was entirely unregulated by the statute or the Constitution and was therefore freely available to government agents. In other words, the decision to read the narrow and device-based statute to cover techniques yielding information analogous to that obtained by pen register and trap and trace devices reflected executive rather than legislative or judicial choices.

The second challenge the reasonable expectation of privacy test raises involves how courts determine what constitutes a "reasonable" expectation when new communications technologies are at issue. One possible approach would be a positive or empirical one, designed to measure *actual* beliefs about the privacy of particular technologies. Apart from the fact that an empirical assessment of such beliefs can be difficult for courts,[122] those beliefs may be influenced by factors that are tangential to the core concerns of the Fourth Amendment. For example, actual societal perceptions about privacy may be based on the positive law protecting communications, the degree to which that law is actually enforced, and even the marketing strategies of those who sell software designed to protect the security of computer systems. A normative approach to measuring privacy expectations—that is, one that asks not what privacy users *do* expect but what privacy they *should be* entitled to expect—may be preferable to a positive or empirical one. The Court's reasoning in *Katz* to some degree reflects this approach,[123] as does the decision of the Sixth Circuit panel in *Warshak*. But even if a court's approach to the reasonable expectation of privacy test should be a normative one, there are a range of interests that a normative analysis could take into account. Discussion of the range of possible interests is beyond the scope of this essay; for now, it is sufficient to point out that *how* courts measure societal expectations will affect the role that courts can play in moderating the security and

---

121 I discuss this issue at greater length elsewhere. See Bellia, 72 Geo Wash L Rev at 1432–33 (cited in note 9).

122 See Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan Tech L Rev 3, ¶¶ 8, 23, online at http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf (visited Jan 12, 2008) ("Courts have either avoided the reasonable expectation of privacy analysis, or have cut short the analysis, because they lack adequate empirical data for the positive inquiry and adequate guidance for the normative one.").

123 As Susan Freiwald has pointed out, the vulnerabilities of the telephone to illegal private and governmental wiretapping were well known at the time the Court decided *Katz*. Id at ¶ 28. See also *Smith*, 442 US at 740–41 n 5 (noting that if influences "alien to well-recognized Fourth Amendment freedoms" have conditioned subjective expectations, normative analysis is required).

privacy interests at stake in communications surveillance. An underdeveloped conception of how to measure societal expectations will privilege executive decisions about the standards and procedures that should govern agents' activities.

My point is emphatically not that the acquisition of communications or other data amounts to a Fourth Amendment event regardless of circumstances. My point, rather, is that the current communications surveillance law framework tends to privilege executive decisions about how to moderate security and privacy considerations, especially when new technologies are involved. The executive is likely to have some institutional advantages over courts in assessing whether national security or other imperatives require government access to certain categories of information, but it has no advantages over courts and legislatures in choosing the standards or procedures that should govern that access.

Indeed, the example of the DOJ's interpretation of how to apply the pen register and trap and trace statute to addressing information associated with electronic communications is somewhat unusual. The Department's general approach to changes in communications technologies has been to attempt to guarantee its continued access to the communications that it has traditionally been able to reach, without altering the legal predicates for access. That position guided the legislative efforts that culminated in passage of the CALEA, which essentially required the telecommunications industry to design its digital equipment so as to preserve law enforcement agents' ability to acquire communications contents and attributes that have traditionally been available in an analog environment. That sort of posture, however, does not account for the new categories of information accessible under or outside of existing legal standards, or the vastly greater volume of information within some of the traditional legal categories. In other words, the government's impulse in seeking not to *lose* access to categories of communications that it could traditionally access is an understandable one, but it does not take account of how dramatically those categories have expanded.

Although not directly related to the requirements of CALEA, the disjoint between Congress's intent in passing the Stored Communications Act in 1986 and the current effect of that statute is particularly telling. Title III codified *Katz* and *Berger*, and in 1986 Congress extended Title III to bar the interception of electronic communications. But Congress treated stored electronic communications in a fundamentally different way. The trends in the cost and density of storage and the structure of the online storage market show why Congress might have done so. Storage was expensive—indeed, *100,000 times* as expensive as it is today. Long-term storage was envisioned to

be a tool of the business community, hence the business-record-like treatment of materials in long-term storage with the provider of a "remote computing service." Congress simply could not have envisioned that long-term storage trends would eventually permit government agents to acquire communications analogous to those covered by Title III, but under far lower standards. As discussed earlier, the SCA distinguishes between communications that are held in "electronic storage" by the provider of an electronic communications service, and communications that are maintained by the provider of a remote computing service, with the former category receiving higher protection than the latter. Even if Congress intended the former category to reach only communications not yet retrieved by a subscriber, evolution of the architecture of memory would now cause the lower legal standard to apply to a vastly greater quantity of information than it reached in 1986.

In other words, the government's approach of seeking to keep pace with technological developments by maintaining its *technical* ability to acquire the same sorts of communications that it could acquire in an analog environment, while maintaining the same *legal* standards for access, may be a reasonable one. But to the extent that it focuses on types of communications while overlooking questions of scale, it begs the question of whether different legal standards should apply.

C. Communications Surveillance for the New Architecture of Memory

Part III.B established that the changing architecture of memory raises critical questions about the substantive standards for access to communications and other information, the procedures or institutional arrangements for implementing those standards, and, above all, the overarching issue of institutional choice. Current Fourth Amendment doctrine, as implemented in the main federal communications surveillance statutes, tends to focus narrowly on surveillance techniques and to assess societal privacy expectations in positive rather than normative terms, with the result that constraints on executive conduct tend to be fairly narrow.

I argue here that the dramatic changes in the architecture of memory require that courts applying the Fourth Amendment to surveillance technique controversies and legislatures seeking to implement or supplement the Fourth Amendment attend to the results of communications surveillance as much as to the methods used. Predigital constitutional baselines for communications surveillance serve as a useful starting point, and we can analyze current surveillance techniques by assessing whether the techniques produce information that is functionally equivalent to information that direct surveillance pro-

duces. We can measure functional equivalence in two ways. Qualitatively, we might consider one surveillance tactic to be functionally equivalent to another if it yields the same type of information, or a different type of information that plays the same role, as information yielded by another method that does have Fourth Amendment implications. The example of demand response technology illustrates the former. In *Kyllo*, the Court assessed use of a thermal imaging device in the same way as it would assess a physical entry into the home because it produced the same kind of information. Similarly, compelling production of information from the utility company yields, in qualitative terms, the same information as entering the home (if not more).

A quantitative measure may also be important in some cases. Assuming law enforcement officials seek to gather information that is functionally equivalent to information previously available in some other form under a *low* constitutional or statutory standard, their activities may raise more concern if they will involve a vastly greater pool of information.

I consider these questions in more detail, focusing separately on communications contents, communications attributes, and transactional and passive data.

1. Contents of communications.

I have already alluded to the possibility that retrospective analysis of communications can produce the same type of communications as prospective acquisition of communications over a period of time. Title III and the SCA, however, treat such information quite differently, and the SCA itself contains multiple standards that some interpret to grant less protection to communications a provider continues to hold after the subscriber accesses them. By qualitative measures, there is no distinction between communications gathered prospectively and the same communications gathered in one or a series of retrospective collections.

There is nevertheless one intuitively appealing reason to distinguish between ongoing, prospective surveillance and a one-time retrospective collection of communications or information. Professor Paul Ohm considers these issues in relation to what he calls a Fourth Amendment "right to delete."[124] The right to delete data, he argues, may account for why email messages implicate the Fourth Amendment's warrant requirement if they are acquired by police in real time, but (perhaps) not if they are acquired from storage: one cannot delete

[124] Paul Ohm, *The Fourth Amendment Right to Delete*, 119 Harv L Rev F 10, 11 (2005), online at http://www. harvardlawreview.org/forum/issues/119/dec05/ohm.shtml.

data as it is transmitted in real time, but one can do so retrospectively. As a result, he suggests, surveillance of information that one has no opportunity to delete is more invasive than surveillance of information that one does have an opportunity to delete.[125]

It is not clear whether this aspect of Professor Ohm's account is intended to be purely explanatory or normative. If it is intended to be normative, there are two difficulties with it. First, the right to delete is by no means complete. With respect to email providers, users have no ability to delete communications that are within the service provider's rather than the user's control. Even to the extent that users do have the technical ability to delete communications, it is unclear that Fourth Amendment or statutory analysis should give that technical ability categorical weight. To the extent that there are competing incentives to retain data, the decision to do so should not be taken as forfeiting any privacy interest. Any other conclusion would permit the subscriber's choice to contract with a provider to store communications to dictate legal standards for producing such communications, thereby distorting the subscriber's incentives. On a related note, users' choices about whether to retain or delete communications are unlikely to be "informed" ones as to the privacy consequences of those choices. In prior work I have discussed the importance of so-called "information structures" in surveillance law—that is, institutional design mechanisms that permit public (and congressional) evaluation of the effectiveness of a surveillance law regime. In particular, I have argued that such mechanisms can serve privacy-protective and law-articulating functions and thus have a special role to play in the context of surveillance practices not subject to prior judicial approval (or subject to judicial approval under a low standard).[126]

One important aspect of the shift from direct to indirect surveillance is that it entails a shift from a regime with a robust information structure to a regime with virtually no such structure. Quite apart from the privacy-protective and law-articulating functions of an information structure, the absence of such a structure can have market-distorting effects that in turn shape data retention practices. Throughout this essay I have focused on the connection between private data retention practices and government surveillance practices, without considering the implications of private party collection and exchanges of data. Arguments against government involvement in regulating the private collection and transfer of data are likely to proceed from the

---

125 Id at 15.

126 See Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance*, 50 Vill L Rev 425, 467–76 (2005) (advocating changes to FISA's information structure).

view that user preferences, and thus an optimal amount of privacy protection, will be achieved through market forces. Even if one accepts this perspective, the lack of information on indirect government surveillance practices will prevent users from signaling concerns about these practices. In fact, in this context consumers face double-layered secrecy: unknown government surveillance practices play off of unknown private retention practices.

2. Communications attributes.

Turning to communications attributes, if we analyze the type of information agents can collect regarding electronic communications, we see that it is a much more expansive category than the phone numbers at issue in *Smith*. Qualitatively, some information associated with electronic communications may be similar in that it performs the same function of allowing the provider to direct the communication. As I have noted, however, if service providers can store communications attributes indefinitely, law enforcement officials can draw data from a larger pool and at any time, rather than simply as the communications occur. In quantitative terms, then, communications attributes involve a significant move away from the constitutional baseline of *Smith*.

3. Transactional and passive data.

Transactional data presents difficulties similar to those presented by communications attributes. Here the constitutional baseline is *Miller*, which at a minimum suggests that business records produced in a customer's relationship with a transactional partner are not subject to a reasonable expectation of privacy. In terms of whether transactional data is qualitatively equivalent to the records at issue in *Miller*, some such data clearly is analogous. For example, purchase of an item online will generate a record of a credit transaction similar to that generated with a brick-and-mortar store. The data, however, may also include data giving rise to inferences that are simply not otherwise available without direct physical observation. For example, a record of a customer's interaction with an online bookseller will include not only the items purchased, but also the items browsed. And to the extent that lower standards might be justified on the theory that the data subject has some control over the data trail—for example, by limiting a site's use of cookies to link information across pages and visits—that control again proves to be elusive. Once created or collected, data is treated as being "owned" by the transactional partner, and any ability to control its disposition depends on the data retention and destruction policies that the transactional partner chooses to implement. As for control over the creation and collection of data itself, the lack of

information on a transactional partner's *retention* practices means that consumers will be unable to make informed choices in this regard.

Finally, the sort of passive data that pervasive computing applications can produce, particularly about events inside the home, will be qualitatively equivalent to direct observations by government agents that are treated as searches under the Fourth Amendment.

CONCLUSION

The changing architecture of memory raises fundamental questions about the application of well-entrenched rules for communications surveillance. An underdeveloped conception of societal privacy expectations and narrowly drafted statutes essentially encourage government agents to exploit the new architecture. The law thus underprotects communications that are functionally equivalent to communications that receive the highest protection under our surveillance law regime. And despite the weak constitutional baselines for communications attributes and transactional data, there are strong reasons, related both to the quantity of information available and the inferences that can be drawn from it, to tweak our current surveillance law regimes to provide heightened protection. I do not contend that the changing architecture of memory counsels in favor of high-level and Fourth Amendment–based protection in all cases. Rather, I argue that courts and legislatures cannot gain a full picture of the surveillance law landscape without accounting for the changing architecture of memory, and that the changing architecture of memory should affect that landscape.