The Digital Individual and the Private Realm

Michael R. Curry

Department of Geography, University of California, Los Angeles

Geographic information systems and the technological family associated with them—global positioning systems, geodemographics, and remote surveillance systems—raise important questions with respect to the issue of privacy. Of most immediate import, the systems store and represent data in ways that render ineffective the most popular safeguards against privacy abuse. But the systems are associated with more fundamental changes in the right to privacy and even, some would say, with challenges to the possibility of privacy itself. They make reasonable and acceptable the view that technological change is inevitable and autonomous, and therefore, too, are the development of increasingly comprehensive dossiers on individuals and households and the use of increasingly powerful means for the technological enhancements of vision. And their use in the creation of data profiles supports a wide-ranging reconceptualization of community, place, and individual. Nonetheless, in the ways they create and use digital profiles, the systems do offer suggestions for a partial remedy to the problems that they have created. *Key Words: geographic information systems, geodemographics, privacy, surveillance, law, technological change.*

The last few years have seen an explosion in the use of geographic information systems. By adding geographical coordinates to the usual elements of an information system, these computerized systems allow not just tabulation and statistical analysis, but also visual representation, especially in the form of maps. These systems are a major growth industry; government and private industry alike have seen them as offering new and powerful ways of making political and economic decisions. But a growing number of scholars have begun to voice concern about the potential impacts of the systems (Curry 1994; Lake 1993; Pickles 1995; Smith 1992). Nowhere has this been more evident than in the matter of geodemographics, a commercial offshoot of geographic information systems used primarily by the direct marketing industry (Crampton 1993; Goss 1993, 1994).[1]

Yet I would argue that those who have examined the social impacts of geodemographics, and of geographic information systems more broadly, have been only partially successful in making clear the potential impacts of those systems on the right to privacy and even on the nature of privacy itself. Granted, critics have pointed to ways in which these systems raise questions with respect to privacy, surveillance, and power. They have shown that when one ties a geographic information system to a global positioning system, and the two to satellite or other remotely-sensed imagery, one has created a system of great power, and of great utility for the storage and analysis of information and for extended surveillance on individuals and groups. Nonetheless, these critiques have not made entirely clear the ways in which the systems raise problems different from those raised by other technologies such as cartography or information systems more broadly. I shall argue that these systems raise new questions about the possibility of privacy, and that certain of their features erode the utility of traditional tools of privacy protection. At the same time, the systems raise deeper concerns. They are associated with an erosion of the traditional forms of the private and the public—and as a consequence require that scholars, activists, and the public at large rethink both realms.

These issues will be taken up in three parts. First, I shall briefly lay out the history of what has come to be known as the right to privacy. We shall see that if privacy itself is a longstanding phenomenon, the codification of privacy as a right is rather new. Further, the nature of that right has undergone substantial changes during its brief history, changes which are directly connected to underlying social and especially technological changes. But those changes—and as a result privacy itself—are often imagined to be autonomous and inevitable. If we see this in popular accounts

Annals of the Association of American Geographers, 87(4), 1997, pp. 681–699

Published by Blackwell Publishers, 350 Main Street, Malden, MA 02148, and 108 Cowley Road, Oxford, OX4 1JF, UK.

of technology, as in works like Alvin Toffler's *Future Shock* (1970; Schwartz 1995), I shall show that recent court decisions have appealed to this very image. In their appeal to a kind of technological "destiny," the courts have naturalized as inevitable the combining of data into dossiers and the use of technological enhancements of vision; these decisions call into question the very possibility of privacy in the traditional sense.

Turning to the current use of geographic information systems and geodemographic systems in the second part, I shall point to several issues that such systems raise. One such issue is the widespread availability of unregulated data; another concerns the ways in which the systems employ visual representations embodying implications about individuals or households; a third concerns the way the data may be incorporated into other databases in a process known as data profiling—a version of data matching that appears to pose new problems to privacy. I show that these features severally and together raise substantial issues about the individual's right to privacy and call into question the very possibility of meeting traditional standards for privacy protection.

In the third part of the paper, I shall discuss the way in which one form of geographic information systems, geodemographics, is associated—through the construction of data profiles and digital individuals—with a reconceptualization of the right to privacy, and at the same time of the nature of the public and the private. On the one hand, the systems involve a reconceptualization of the nature of culture and place. Cultural groups are represented as mere aggregations of individuals in a way that undermines the legitimate claims of those groups. Individuals are conceived of as belonging to groups only by virtue of having certain socioeconomic characteristics or personal habits; to remain a part of a group does not require that one behave in some way toward one's fellow members, but rather that one maintain those socioeconomic characteristics. And places are seen as locations to which individuals are only contingently attached. Here, the traditional practices of place formation and sources of attachment to place disappear and here, again, to be a part of a place is simply to maintain the right set of socioeconomic characteristics.

On the other hand, the creation of data profiles involves a reconceptualization of the individual, and in a complex way. At least through the 1980s, it was usual to attack the creation of comprehensive dossiers on individuals on the basis of a belief—ironically, consistent with the postmodern conception of the individual—that individuals ought to be able to compartmentalize their lives, and ought not to be held accountable in one area for things that they have done in another. But the creation of data profiles seems to call an end to this postmodern view, asking that it be replaced with an older, modernist view in which individuals are seen as coherent units that share visible and quantifiable characteristics with their neighbors.[2] With data profiling, it appears possible to draw a wide range of inferences about any individual, inferences that cross boundaries that were until now closed.

If this suggests that we are moving inexorably into an ominously surveillant world, I shall suggest that with the virtual or digital individuals created by data profiling, geographic information systems contain the seeds of the destruction of that surveillance. If they are a problem, just to the extent that there are so many of them and that they are seen by so many people, they offer a solution: each of us ought to be able to control just what our virtual selves do—where they go, what they say, and to whom they say it. To rethink privacy in this way is to recapture important elements of the postmodernist understanding of privacy. It is at the same time directly to connect the issue of privacy to the Hegelian and European tradition in intellectual property regulation. In this way, we may adapt the concept of privacy to the world created by geographic information systems.

Technological Change and the Changing Right to Privacy

On the Genesis of the Right to Privacy

The formulation of the explicit right to privacy has its origins in urban society in the late 1800s. Before that time there was no well-enunciated privacy right; certainly people had privacy, but it was guaranteed by the existence of a landscape within which certain practices could by and large be expected to be private (Friedman 1990). But the economic and technological transformation of that landscape in the late nineteenth century solidified the distinction between the urban and the rural. And in doing so, it set the stage for the formulation of privacy as a right.

The urban, as Georg Simmel bemoaned in his famous "Metropolis and Mental Life" (1971

[1903]) and Louis Wirth later formalized for American urban sociology (1938, 1969), became a place in which an individual could choose to remain isolated and anonymous. The problem for privacy created in this new landscape, where the actions of the individual seemed so little constrained by custom, was solved by the development of a formalized set of privacy guarantees, as set out in a famous law review article near the end of the last century. There Warren and Brandeis (1890) asserted that the individual has a right to privacy, where that is the right "to be left alone."

If it has been common in thinking about the individual, at least since the 1650s, to imagine the individual as having a single, coherent identity, there is a sense in which popular practice during the era after Warren and Brandeis took a very different tack, one more consistent with the views set out by Simmel. Not only was the modern urban individual seen as living a fragmented existence, that fragmentation was seen as beneficial, and as something that needed to be supported.

Written one hundred years before Warren and Brandeis, the U.S. Constitution does not itself enunciate a fundamental right to privacy. But it does in various places lay out what many scholars have regarded as elements of such a right. The Fourth Amendment, concerning searches and seizures, is one such element. It states that:

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

This amendment limits the actions of government. It does so by stipulating that there are certain cases in which a government (typically in the form of the police) may not engage in searches or take the fruits of such searches without first obtaining the assent of a putatively more neutral third party (typically in the form of the judiciary). Indeed, it *defines* searches as those cases in which such assent, in the form of a warrant, is necessary.

With respect to the genesis of this amendment, one can tell a long story, as David Flaherty has (1967), but there is general agreement about a shorter version of that story (Amsterdam 1974; Gutterman 1988; Tomkovicz 1985). On this view the amendment arose from a perception of abuses by the British government, particularly its practice of issuing unrestricted warrants. The right to privacy since that time has been closely connected to the ability to restrict the sorts of information that is publicly available. Finally, privacy has continued to be seen as having important social functions; it is commonly seen as essential to the spiritual and personal development of the individual and the family, and hence as indirectly important to society more broadly.

New Technologies and the Changing Private Realm

At the time of the writing of the Constitution, the house was seen as the central locus of intimate activities, and hence as the place where the intervention of the government needed the strongest justification. But if so, in the U.S. it was assumed—in keeping with common law—that what was important was less that area bounded by four walls than the somewhat larger area within which the intimate activities of everyday life took place; this "curtilage" consisted of (as the Oxford English Dictionary put it):

> A small court, yard, garth, or piece of ground attached to a dwelling-house, and forming one enclosure with it, or so regarded by the law; the area attached to and containing a dwelling-house and its out-buildings.

As late as 1924, Justice Holmes alluded to the curtilage in *Hester v. United States*; turning for authority to Blackstone's *Commentaries*, he distinguished between the dwelling-house and curtilage, and the "open fields" beyond, claiming the distinction to be "as old as the common law" (1924:59).

Means, Ends and the Changing Nature of Privacy. But a variety of social, economic, and technological changes have, over the last hundred years, seemed to widen the arena within which the presumption of a right to privacy ought to operate. Over this period, the area within which private activities can take place has been extended beyond the home and curtilage, to the workplace, the automobile, and even the telephone booth. Yet these extensions have not been simple or uncontested. Some have held that when we apply the Fourth Amendment to new circumstances, we need to ask the following question: Are the actions of the government here physically like those used in making a "tradi-

tional" search of a house? Others have asserted that we need to ask a different and more encompassing question: If we were to deny that a telephone booth, for example, can be a place within which people have a right to privacy, what would be the impact of this denial on the values that the Constitution was designed to protect? Some, then, have believed that the essential issue with respect to the actions of government is the means used, while others have argued that we need to look at the ends that we—and the Constitution—seek (Amsterdam 1974).

It is useful to couch the discussion of privacy in recent court decisions, and especially decisions of the U.S. Supreme Court. The courts do have an impact, but more important, the Court's thinking on this issue can be seen as mirroring views more widely held. Indeed, I shall argue that recent Court decisions reflect conceptions of culture and of technological change that are in accord with those implicit in practitioners' thinking about geodemographics and geographic information systems.

In fact, over the last hundred years, the Supreme Court has wavered between these two poles, for a time appealing to an ends-based view, then a means-based view, and sometimes claiming to take one view while appearing to take the other.[3] On one side, we find a trend begun in *Boyd v. United States* (1886:630), which maintained that a person's Fourth Amendment right could be violated even absent a physical search: "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property. . . ." What is important is not the means used, but rather the values or ends that might be violated by the action of the police.

On the other side is the view taken in *Olmstead v. United States* (1928:465–66)—a wiretap case—which held that:

> By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. . . . The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. . . .

On this means-based interpretation, a wiretap involves no invasion of privacy, since there has not been:

> an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house "or curtilage" for the purpose of making a seizure.
>
> We think therefore that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment (*Olmstead v. United States* 1928:4666).

Later courts elaborated on *Olmstead*'s means requirement of a real, physical search by appeal to the threshold conditions defined in *Hester v. United States*. There the Court decreed that:

> the special protection accorded by the Fourth Amendment to the people in their "persons, houses, papers, and effects," is not extended to the open fields. The distinction between the latter and the house is as old as the common law (*Hester v. United States* 1924:59).

Olmstead's means-based decision that wiretaps were not searches was taken to be the law until it appeared to be reversed in *Katz v. United States* (1967). There the Court appeared to buckle under the weight of technological change and reversed itself in a way that looked back to the values- or ends-based thinking in *Boyd*. It argued that even within a public telephone booth, a person's right to privacy could be violated, simply because by closing the door, the individual feels justifiably isolated from the public world outside. And, indeed, as we shall see in what follows, the courts today generally take *Katz* to have overturned *Olmstead* and to have provided a way of dealing with the issue of privacy that much more effectively negotiates a world of ever-present technological change.

From Individual Facts to the Big Picture. Still, certain cases have indicated a failure to appreciate the nature of such change. In one set of cases, for example, the Courts dealt with searches that uncovered small "bits" of evidence. In *Smith v. Maryland* (1979), in fact, was laid out what has come to be the guiding interpretation of *Katz*, albeit one which draws not from the Court's opinion itself but rather from Justice Harlan's concurring opinion. In *Katz*, Harlan argued that a search has been carried out under the terms of the Fourth Amendment when the situation meets "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' " (361).[4] In *Smith* the issue was a pen register installed by the telephone company to record the telephone numbers that had been dialed from the petitioner's home. (Such a system was required before the development of modern computerized switching systems.) Smith contended that the acquisition of that list by the telephone company constituted a search. But in *Smith*, the Court decreed first that "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial (742)." Moreover:

> even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as 'reasonable' " (*Katz v. United States*, 389 U.S., at 361). This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties (743–44).

In a more recent case, *"United States v. Place"* (1983), involving the use of trained dogs to sniff for drugs, the Court concluded that the privacy interests of the people involved were not threatened because the dogs in question were capable of discovering only one thing, cocaine. The Court reasoned that the violation of privacy required the collection of a larger range of information.

The issue that these and like cases raise, in the context of information systems generally and geographic information systems more specifically, is this: What happens when each of these individual items of information is combined into a larger dossier? One commentator on the issue of searches suggested the following:

> If a police officer, seeking to learn whether my car is in the garage attached to my home, lies down in my driveway and shines his flashlight through the half-inch gap between the bottom of the garage door and the garage floor, I would be annoyed somewhat by his choice of method, but my ultimate reaction would be, "So what's the big deal?" (Fishman 1988: 349–50).

There might not be a "big deal" if this action were merely carried out occasionally by a person who kept the information in his or her head. But once each individual item of information can be incorporated into a larger, geocoded information system, the situation changes; in a fundamental sense, it no longer makes sense to talk about a single-function inquiry: The telephone numbers in *Smith* and the cocaine-sniffing dog in *Place* can become elements of a much larger system.

Autonomous Technology in the Courts

In this and other recent cases, it is helpful to see the Court's vacillation about the relative importance of means and values, and its difficulty in understanding technological change, as expressive of an underlying set of assumptions about such change and about the nature of society.[5] From its view, change is neutral and autonomous. To make the statement that technologies are seen as neutral is to say something rather simple; that is, that any impacts of a technology derive from its use, and not from some features inherent in the technology itself. Well ensconced in public discourse, this is the view that "Guns don't kill people; people kill people."

The term "autonomous technology" may be less familiar, but the concept is no less prevalent; it is the view that:

> Technique has become autonomous; it has fashioned an omnivorous world which obeys its own laws and which has renounced all tradition. Technique no longer rests on tradition, but rather on previous technical procedures (Ellul 1964:14; see also Winner 1977; Street 1992).

Hence, to believe that technologies are autonomous is to believe that they contain their own logics, their own trajectories. The development of a technology occurs in a way preordained; disk drives become larger, global positioning systems become more accurate, CPUs become more powerful, all not because of human decisions, but rather because once the object comes into existence, once it is invented, those changes are built in; they are, in a way, part of the essence of the object.

The literature on the history, sociology, and geography of technology is filled with critiques of these two views; indeed, it is probably fair to say that few in these disciplines would today hold the belief that a technology can be neutral, and fewer still would believe that technology is somehow autonomous. Nonetheless, the success of the courts in laying out these views suggests that they are broadly held. And more important, by defining the law as though technologies are autonomous, court decisions institutionalize that way of thinking and render it more true. Unfortunately, in the context of the conflict between means- and

ends-based interpretations of privacy law, this way of thinking has several untoward consequences.

The Enhancement of Vision. That technology holds profound implications for what constitutes the private sphere is especially seen in a set of cases directly relevant to geographic information systems because of their use of remote sensing. Here the issue is the use of technology to enhance normal means of search. In a series of cases—*Dow Chemical Co. v. United States* (1986); *California v. Ciraolo* (1986); *Florida v. Riley* (1989); *United States v. Penny-Feeney* (1991)—the courts have shown their willingness to entertain the use by law enforcement of increasingly powerful technologies, ones that call into question what some have seen as a clear boundary between curtilage and open fields, and which thereby shrink the area that can be called "private."

The common-law distinction between the curtilage and open fields had in part defined those areas within which evidence could be taken at will and those in which the Fourth Amendment requirement for warrants needed to be met. Even within the curtilage, those actions which remained open to view remained public; the police, it is often averred, need not shut their eyes when looking at someone's house or yard. But if the curtilage remained subject to the gaze of the public, it was nonetheless possible to render it private, by taking the requisite steps, like planting trees or shrubs or erecting a wall or fence. In *Ciraolo*, though, the Court decreed that changes in technology can require that people take further steps. In that case, the police flew over a fenced-in backyard at an altitude of 1,000 feet and were able to identify marijuana plants growing in the yard. The Court held:

> That the area is within the curtilage does not itself bar all police observation. . . . Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible (*California v. Ciraolo* 1986:1812).

They continued,

> Any member of the flying public in this airspace who glanced down could have seen everything [i.e., marijuana plants] that these officers observed. On this record, we readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor (1813).

In *Dow* (rendered the same day), the Court made a similar finding, but with respect to an industrial site.

Then, in *Riley*, the Court went further. There the police had used a helicopter, hovering at 400 feet, to observe marijuana plants through a hole in the roof of Riley's greenhouse, which was located in his backyard. As in *Ciraolo*, the Court concluded that "Any member of the public could legally have been flying over Riley's property at the altitude of 400 feet and could have observed Riley's greenhouse" (451). And a Hawaii District Court went even further, in *Penny-Feeney* (Steele 1991, 1993). There police in a helicopter used a FLIR (forward-looking infrared device) to discern heat emissions from a garage, within which they believed that marijuana was being grown, aided by heat-emitting grow lights. On the basis of the photographs, they obtained a search warrant.

If, in *Penny-Feeney*, the police went beyond the usual binoculars and flashlights, two rather different cases raise this same issue of sense enhancement in the context of a different technology. In *United States v. Knotts* (1983) and *United States v. Karo* (1984), police used beepers to identify the location of individuals. The beepers allowed them to track the individuals for long periods, developing a story about where and with whom they (and their drug-producing, beeper-laden cargo) had been.

Each of these cases is slightly different, but what they have in common is the use of technologies—helicopters, airplanes, FLIRs, beepers with radio direction finders—which belong to a technological "family." In the case of the beeper, a geographic information system would allow not just tracking but mapping of the automobiles involved. In the case of *Dow*, the cameras used *were* mapping cameras. In *Penny-Feeney*, the technology used is the very technology used in satellite remote sensing. And in *Ciraolo* and *Riley*, the principles used are indeed those of remote sensing. In each case, the technological devices are used to enhance normal vision, to make visible what was previously not. The courts have traditionally drawn a line, not allowing the government to use technologies not readily available to the public. But here the courts seem to be accepting the view that as what is "readily available" changes, so too does the nature of the technology that the government can use.

Here, as in the cases above of beepers and drug-sniffing dogs, the courts have argued as though technological changes are natural, and as though everyone ought to accede to them—and rethink the right to privacy. And here, too, that rethinking has generally been in the direction of diminishing the power of the individual and increasing the power of government.

Autonomous Technology and the Reasonable Expectation. This returns us to the issue raised in *Katz*, the nature of reasonable expectation. Appealing to the *Katz* criterion for the "reasonable expectation of privacy," the Court has interpreted "reasonable expectation" in a way that allows the reasonableness of that expectation to change along with technological change. Granted, the Court has not to date allowed the introduction of satellite imagery into domestic cases (although certainly these images are used internationally, and used by the U.S. government in its anti-drug program in Latin America). But as the resolution of images becomes better and costs lower, these images may very well become so common that it will make sense to argue that the use of them by police is consistent with popular practice. Indeed, the rapid and widespread adoption of global positioning systems and the development of private satellite systems, expected within two to three years to be producing commercially available images with a resolution of one meter, suggest that this may not be so far off as many on the Court have believed. Yet to say that popular practice may involve the widespread use of global positioning systems and of remote sensing is not at all to say that people will take the results of those practices to be reasonably expected.

In fact, to say that society is prepared to accept something as reasonable is at once to make a complex decision. It is to appeal to a corporate body, "society." It is to ask of that body that it envision something about the future. And it is to ask that it render a judgment about that future. Nonetheless, in a concurring and influential opinion in *Riley*, Justice O'Connor without comment redefined the *Katz* standard of what "society is prepared to recognize as 'reasonable' ":

> If the public rarely, if ever, travels overhead at such altitudes [400 feet], the observation cannot be said to be from a vantage point generally used by the public and Riley cannot be said to have "knowingly expose[d]" his greenhouse to public view. However, if the public can generally be expected to travel over residential backyards at an altitude of 400 feet, Riley cannot reasonably expect his curtilage to be free from such aerial observation (*Florida v. Riley* 1989: 455).

If the two statements in *Katz* and *Riley* seem similar, note the differences: *Katz* referred to "society" as a corporate body; in speaking of the public traveling over backyards, O'Connor is surely talking at most about groups of individuals. *Katz* referred to what society is "prepared" to accept; O'Connor referred to what people in fact do. And *Katz* referred to the "reasonableness" of the expectation; O'Connor, again, referred to people's behavior.

In effect, O'Connor suggests that we can read off society's preferences from the current state of society and that we should see society simply as an aggregate of individuals. The first suggestion, which derives an "ought" from an "is," is simply silly; one need not read the critical literature on revealed preferences, but need only look around to find that individuals do not at all accept as reasonable a great deal of the ways things are. Certainly it makes little sense to deduce from the fact that one often hears helicopters overhead the conclusion that people see this as reasonable, and equally see as reasonable that what they do in their backyards or even their homes is in plain and open view. Here it is the implicit belief in autonomous technology, the belief that this technological change is occurring in a natural way, one intrinsic to it, that allows the easy conclusion that the changes are to be "reasonably expected."

This theory has allowed the courts to avoid confronting the consequences of these technological changes for the very practice of government. For example, there is in government offices today a huge store of data that are available to the public, and some of these data are now being incorporated into information systems, including geographic information systems. There is a tendency to see this incorporation as failing to raise any important issues, simply because the data were always available. But it is important to recognize that the decision to make those data freely available was made when "freely available" meant something very different from what it now means; the people who supported laws making certain kinds of data available understood the operation of those laws only in terms of the technologies available to them, and the regulations were almost all written before the development of computers and geodemographics.

In concert with the courts' implicit theory of technological change, this failure to look beyond the individual to the social and cultural value of privacy is particularly dramatic. The courts have allowed first this, then that diminution of the arena within which a person can see her behavior as truly beyond surveillance, but have imagined that no structural change will grow out of the sum of those individual changes. This has led the courts to imagine that a society in which everyone's actions are under constant surveillance will be no different from one in which only some are sometimes under surveillance (Granholm 1987). While explicitly embracing the ends-based *Katz* interpretation of the Fourth Amendment, the courts have in fact been basing their opinions on a view in which technological change is seen as neutral and autonomous; they have deferred to a means-based view wherein means and ends are increasingly the same.

On the Value of Privacy

Of course, most of the recent privacy-related cases that the U.S. Supreme Court has decided have concerned activities—like drug smuggling (but also terrorism and child pornography, together often invoked as a kind of mantra in computer-network-related cases)—that have a sordid side. Few in the public are galvanized to protest by the sight of a drug smuggler being sent off to prison. And indeed, for this very reason many people simply shrug off the changes that have been occurring in the legal definition of the right to privacy, and hence of the institutionalized definition of the private realm itself. Further, some, seeing themselves as hard-headed, have argued that the appeal to the private is simply nostalgic, a sign of a kind of mental illness. And finally, some have argued that since any privacy regulation is certain to work to the benefit of the wealthy—one (apparently) apocryphal story has it that the original Warren and Brandeis article grew out of their distaste for the paparazzi—we ought just to give it up, to live lives that are transparent to all.

Yet a bit of reflection suggests the difficulty with all of these positions. The difficulty is, putting the matter simply, that the private realm performs important functions in the life of the individual and the group. It is in private that people have the opportunity to become individuals in the sense that we think of the term. People, after all, become individuals in the public realm just by selectively making public certain things about themselves. Whether this is a matter of being selective about one's religious or political views, work history, education, income, or complexion, the important point is this: in a complex society, people adjust their public identities in ways that they believe best, and they develop those identities in more private settings.

As scholars we are all well aware of this. Few of us, after all, would wish every draft of every paper and lecture to be open for public scrutiny. And we are aware of it as political beings; in a society in which political power is unevenly distributed, the possibility of the less powerful becoming more powerful depends on the possibility of private activity. The ability to engage in these adjustments is contingent on the possibility of there being private places in which the elements of the identity can be assembled and tried out. And it is contingent on there being some realm of private data. Just as we rely on the possibility of doing things in places that are out of sight, we rely on the possibility of some facts about us drifting out of sight after the passage of time. We all assume that there are things about us that others will forget, and we are thereby able to feel that we live in a society where there is the possibility of redemption (Reiman 1984; Schoeman 1984).

What I have said of the individual applies, too, to the group. The creation of a group is contingent on the development of a border, a boundary between the member and the nonmember, the included and the excluded. If, in American society, the discourse about the privacy of groups is less well theorized—indeed, to most the idea of "group privacy" seems almost an oxymoron—the idea is nonetheless embedded in everyday life. Political and religious groups wish to plan and pray in private, and to have some sense of control over the image that is propagated of them.

The refiguration of what counts as a right to privacy, then, has the potential of having important consequences at a variety of scales. So in the context of a general acceptance by jurists—not to mention the computer software and hardware industries—of the inevitability of the technological change that feeds the redefinition of the right to privacy, it is all the more important to understand the potential implications of these changes. As I shall argue, geographic information systems and geodemographic systems have the potential to effect changes in this right in a number of ways.

Geographic Information Systems, Geodemographics, and the Assault on Privacy

If geographic information systems have a wide range of uses, some well outside of the normal practice of geography, geodemographics seems—despite the name—to fit well within the usual concern of geographers. Combining census and other areally coded data with data about individuals and households, geodemographics creates social, cultural, and economic profiles first of areas and then of their residents. These profiles are useful for site selection and political redistricting, and for drawing inferences about the households and individuals in a particular area.

The development of these systems since the late 1970s has been boosted by the growing availability of inexpensive computers with large-scale storage capabilities, and by the accompanying proliferation of computerized governmental and commercial databases. Governments in some countries have supported this development by supplying inexpensive databases; within the U.S., the Postal Service has gone so far as to offer economic incentives to large-scale direct-mail campaigns. They have, for example, provided change-of-address information to help direct marketers keep their lists up to date and even assisted marketers in obtaining complete lists of households in an area (Branscomb 1994). With this aid, a number of companies have developed comprehensive geodemographic systems. In fact, one, Claritas, has been so successful that it has been the subject of popular books (Larson 1992; Weiss 1988).

These systems are, in one sense, quite unexceptionable. Their aim is simply to characterize areas or regions of people with similar lifestyles, based on the assumption that people tend to live in close proximity with others like themselves. The characterization is, by and large, an inductive one; large amounts of data are fed into a computer, and using numerical taxonomic methods, a vast number of places are grouped into a smaller number of large areas.[6] In the first-generation systems, the U.S. was subdivided into geographic areas of 200–300 households each, each of which was characterized as belonging to one of perhaps twenty to forty basic types. Newer, microscale geodemographic systems use the same methods, but produce areas at much smaller scales, in some cases with as few as five to fifteen households. And the newest systems promise to operate at the scale of the "rooftop." In either system, marketers claim to be able to target their campaigns more efficiently at regions of a particular type, thereby saving money, aggravation, postage, and trees.

Described in this way, these systems seem quite benign, but because of the ways in which they treat information about individuals and households, they nonetheless have been a source of anxiety, a new version of one prevalent in the 1960s and 1970s. Then, as computers became more powerful and readily available, people began to worry that governments might, using common identifiers like social security numbers, combine disparate data files into single comprehensive dossiers on each individual. Concern about the possibility of this process of data matching led in the U.S. to the passage of the Privacy Act (1974), the Computer Matching and Privacy Protection Act (1988) (which applied only to government data), and to other, more specific legislation such as the Video Privacy Protection Act (1988). These acts are widely concluded to have been ineffective, largely because they allow for exceptions when matching or other data use can be classified as "normal and routine," and because what is normal and routine has been so broadly construed; as Marx and Reichman said of the 1974 Act, "Broad interpretations of 'compatible purpose' have made it possible to include nearly any government-initiated venture" (Marx and Reichman 1984:440).

Geodemographic systems do, in part, use data matching—they are exempt from the legal controls of the Computer Matching and Privacy Protection Act because they are not governmental—but more important, they use a new version of data matching called data profiling. There the key used for connecting databases is not the social security number, but the geographic coordinate. Geodemographic systems begin with data aggregated at an areal scale, and then typically associate those data with data about individuals or households. The association involves two steps. First, a marketer acquires information on individual purchasing habits, automobile and home ownership, voting preference, religion, and so on. Second, these data are combined with areal socioeconomic data in order to create an areal profile of residents' "lifestyles." It is here, some would suggest, that the users of these systems run up against the issue of privacy. It is not hard to imagine various situations in which a person's right to privacy may be violated, and here, to

alarmists like Larson (1992), images of Big Brother and of *1984* come all too easily to mind.

Even in the absence of effective legislation, it might in principle be possible to deal with certain of geodemographics' potential threats. In the U.S., for example, it is typical to argue that those who find their privacy rights violated can find recourse by filing a civil suit. And other countries have developed a wide range of means of protection, including data protection commissioners, ombudspersons, and the like (Flaherty 1989; Bennett 1992). What many of these remedies to assaults on privacy have in common is an adherence to what have come to be termed "fair information principles (or practices)." Codified during deliberations on the 1974 Privacy Act, these principles assert that the existence of any system of information must be publicly available knowledge, that individuals ought to have access to data about themselves and ought to be able to correct erroneous information, that personal data ought to be collected only where necessary and used only for the purposes for which they were collected, that personal data ought not to be disclosed to another group or agency without some sort of consent, and personal data ought to be protected.

Whether in a U.S.-style tort and civil liability system, in a system based on the registration of databases with government officials, or in a system based on an ombudsman, many would argue that these principles establish a set of criteria that any privacy-protection system ought to meet. But there are three ways in which geodemographics and geographic information systems more generally call into question the possibility of adherence to these principles.

Undisciplined Information

The first limitation on these privacy remedies is related simply to the widespread use of the systems. A quick glance at magazines like *American Demographics* or *Direct Marketing* will show that the systems I have listed in Table 1 constitute only a fraction of the large and growing number of suppliers of demographic and geodemographic data in a large variety of types. The sorts of data used in geographic information systems and geodemographics have become such valuable commodities that skeptics have made a variety of attempts to regulate them while producers have pressed (often successfully) for special treatment for an industry that they regard as central to America's economic well-being (Curry 1996a). The fact that a range of organizations, from the Council of Europe to the European Community to the Organisation for Economic Cooperation and Development (OECD), have attempted to regulate the flow of data underlines their importance (OECD 1976; Commission of the European Communities 1992a, 1992b; Council of Europe 1973, 1981a, 1981b, 1986). So too does controversy raised in 1996 as the World Intellectual Property Organization—with U.S. government support—attempted to establish new and sweeping rules for the protection of databases (Greene and Rizzi 1997).

It is easy here to imagine that something very simple is going on, and I think many casual critics have been misled by a dated and anachronistic image of computers. This image was born in the 1960s and nurtured in the 1970s in a series of reports on the threat posed by computers to individual privacy (*Columbia Human Rights Law Review* 1973; Rule 1973; Westin 1972). These reports expressed widespread fears that the government would build substantial databases of dossiers on individuals and that the computer would facilitate this task by allowing the combining of separate files into larger dossiers. This fear has given rise to a guiding image of the Benthamite Panopticon, where all is visible from a central point (Bentham 1791).[7]

But the fear of the Panopticon was based on an authoritarian image of the computer as a large, expensive, and technologically complex machine accessible to but a few. Since the early 1980s, however, the reality has been very different because of the extraordinary proliferation of inexpensive computers. This reality was driven home several years ago in the case of Lotus Market-

Table 1. Some Current Geodemographic Systems

System	Vendor
Atlas MarketQuest ™	Strategic Mapping
DNA™	Metromail: R.R. Donnelley
Lifestyle Selector	National Demographics and Lifestyles
MicroVision®	Equifax National Decision Systems
Niches™	Polk Direct
Prizm®	Claritas NPDC
Solo®	Trans Union

Place™. This product was a CD-ROM-based system that would have provided data on seven million of the nation's businesses and 120 million of its households. Promoted as a means of providing small and medium-sized marketers and mailers with information long available only to large corporations, the business version of MarketPlace™ was introduced in the autumn of 1990, with the household version expected to follow in the winter of 1991 (Bain 1991; Huber 1990). It was not to be; as one newspaper reported:

> The introduction of Lotus Development Corp.'s Lotus MarketPlace: Households database is being halted because of unusual pressure from consumer and privacy advocates. The software publisher decided that the database . . . is not worth the controversy. Over 30,000 people have called Lotus and demanded that their names not be included on the database (O'Connor 1991: C1).

Many saw this argument as silly, aimed as it was against data that were already available (Seymour 1991; for later analyses see Culnan 1991; Gurak 1995, 1994). But those who objected to Lotus MarketPlace™ had a point—with this system, we were discarding the old view of a centralized computer in the hands of Big Brother and replacing it with something much worse. With a centralized databank, it was at least possible in principle to locate each piece of data about an individual and to correct or delete those data that were incorrect. But that is impossible in the current situation; no one can hope to know who has which data about a household or individual or who has outdated or inaccurate data. If it is difficult to recall defective automobiles, it is even more difficult to recall every CD-ROM, every backup copy, and every map and table that includes infringing data. In the end, all that Lotus was able do for those 30,000 people who wished their names to be excluded from MarketPlace™ was to tell them that their names would be excluded from future editions. The data already in the hands of consumers were there for good. Indeed, the case of Lotus MarketPlace™ shows that our worry ought not to be the Benthamite Panopticon, but rather the "Mirror World" envisioned by David Gelernter, where anyone can see any part of the world, at any level of detail, at any time (1992).

The Power of the Visual

If this problem of undisciplined information is intrinsic to geographically based systems, it is not exclusive to them. One can see the same difficulties with any information system, including radio and the newspaper. But a second feature of the systems, their reliance on the visual, sets them apart from other information systems and creates a second limitation to traditional privacy remedies. Here the problem arises from the way in which visual representations are "read."

In the first instance, this difference arises because those who produce geodemographics use their analyses to characterize neighborhoods or areas in terms that by and large suggest that those neighborhoods are homogeneous. The areas are typified in colloquial and highly general terms, as "Hard Scrabble" (PRIZM®) or "X-Tra Needy" and "Zero Mobility" (Niches™) or "Low Income Blues" (MicroVision®). While these names may not be perceived as a problem, one wonders who would not feel slighted to find that his or her neighborhood was titled "Zero Mobility" rather than "Working Hard" or "Very Spartan."

A version of this problem arises in the analysis of statistical data referred to as the "ecological fallacy." The fallacy is committed when the analyst or reader assumes that the average individual within an area represents any given individual therein. Because the ecological fallacy is a way of thinking with which anyone who publishes statistical research must contend, some might argue that there is no reason to single out visual representations produced within geodemographics. But there is in fact a difference between the commission of the ecological fallacy in statistical work where results are displayed in, for example, tabular form, and its commission in the case of mapped data. This is because people tend to see maps as direct representations of reality in ways that tables and charts are not. There is ample evidence of this. We see it in the ways people misread conformal projections, inaccurately concluding for example that Africa and Greenland are of similar size. Within geography, cartographic theorists have made a similar assumption; they have believed it possible to develop schemes of map representation that the average person can read directly, and without interpretation or error. As Robinson put the matter,

> Your main objective in designing a map is to evoke in the minds of viewers an environmental image appropriate to the map's purpose. . . . [So] When designing a thematic map, you must be sure that the modulations of marks and symbols you choose work together graphically to evoke the overall form of a distribution (Robinson et al. 1995:316–17; see also

Dent 1972; Flannery 1971; Castner and Robinson 1969).

Indeed, until very recently, this view was the law of the land in the U.S. It was only in the 1992 District Court decision in *Mason v. Montgomery Maps* that the courts for the first time held that differences among maps might have an impact on the perception of the data on those maps; previously they had held that differences among maps of the same subject were merely decorative and inessential, and that any two map readers would "see the same thing" when looking at a map (*Mason v. Montgomery Maps* 1992; Wolf 1992, 1993).[8]

Here, then, the issue of privacy is raised not simply because data are uncontrollable, or may contain factual errors about individuals. Rather, concerns arise just to the extent that it is possible to produce visual representations that any reasonable reader will directly read as associating characteristics of behavior or belief with individuals or members of households. In an important sense, such maps paint their subjects, and in colors that may be inaccurate or damaging, that may impute to those subjects behavior or beliefs that they maintain should remain out of the public eye. One might reply that the danger here is not merely with geographic information systems or geodemographics, but with maps or visual representations more generally. This misses the more critical point, that the ease of computer mapping, combined with the increasing availability of data sets, has made maps more readily available and made the possibility of privacy infringement much more likely.

Data Matching and Data Profiles

Beyond the spread of undisciplined data and the ready appeal to the visual, geodemographic systems pose a third threat to the traditional means for the control of infringements of the right to privacy. This is through their use in the construction of data profiles. One of the earliest concerns raised by computers was that of data matching. To prevent the creation of large dossiers on individuals, proponents of the Computer Matching and Privacy Protection Act of 1988 intended that the Act, at least in the arena of the government, make the merging of databases more difficult. Yet geodemographics makes it possible to merge databases in a way that circumvents the law. These systems enable a user to create a profile of an individual not by the collation of individual data across government agencies, but rather by combining individual data with other publicly-available aggregate data, data geographically coded at the level of census block groups, postal carrier routes, and rooftop geocoding. Using a wide variety of characteristics and data that are publicly available, one can create a very probable image of a person.

So in an important sense, the development of data profiling, where those profiles are attributed to individuals, portends an urban environment in which it is possible that any person I telephone will, beginning with a Caller ID system (or the Automatic Number Recognition equivalent, standard with toll-free telephone numbers) be able to identify my name, address, and demographic profile. It may well be an environment in which those in "better" neighborhoods automatically get faster customer—or even emergency—services. And it is equally possible that systems be set so that calls from people with some profiles are not answered at all.

As a result, the use of data profiling undercuts the possibility of privacy (as do the development of undisciplined information and the use of visual representations) to the extent that it renders it difficult to apply the set of fair information practices mentioned above. Indeed, in a geodemographic world, where profiles are constantly being created, marketed, and recreated, it is hard to see how any individual today can know whether he or she has adequate knowledge of which data exist, has access to those data, has the ability to correct those data, or can be assured that data have been collected only where necessary.

Rethinking Culture and the Individual

There is a third very general set of effects of the GIS family on the right to privacy. As in the case of technological change more generally, we see here a set of forces that are not acting simply to render it more difficult to protect the privacy of individuals. Rather, we are seeing forces that are restructuring fundamental features of the social world. In a geodemographic world, we see an ongoing reconceptualization of the objects that make up the world. Social and cultural groups are redefined as mere aggregations of individuals. Places are defined as locations to which are at-

tached merely contingent sets of features or attributes. And cultures and places come to be seen as composed of or inhabited by individuals whose names and bodies come increasingly to be armatures to which are attached geodemographically constructed identities.

Perhaps most obvious here is the redefinition of the relationship between the individual and the group. In order to understand what I mean, it will be helpful first to ask just what the relationships among members of a group and between them and the group might be. There are, of course, a variety of alternatives. In some cases, we feel justified in believing that we have no relationship with some people, other than that we are people. This would be true in the extreme if we were to find our names on a list randomly chosen from the names of everyone in the world. We likely would wish to say that we have a closer relationship with all those people with whom we work, or with whom we share a bus or airplane. We may feel that we have little connection with them, but it remains that we *are* connected just to the extent that we are sharing that vehicle with them.

Many people would argue that with some people, they have much closer relationships. Many, for example, see those in their families or their hometowns or churches or even their workplaces as so close to themselves that "they are part of me." As Eric Voegelin (1940) showed in the case of political bodies, this idea of the intrinsic relationship of the individual to the whole is a long-standing one. Whatever the disadvantages of this idea, it remains that the sense of belonging in some intrinsic way to a larger body, whether a nation or a neighborhood, has long been a critical part both of the individual's motivation to act in some larger interest and of the group's ability to exhort the individual to such actions.

But geodemographics and geographic information systems, like other similar sets of tools, offer a different image of the relationship between the individual and the place or group. Within a geodemographic system, "lifestyles" are the units to which one belongs, and that belonging is strictly a contingent fact. A lifestyle is, after all, nothing more than a statistical aggregation. True, these lifestyles are increasingly described with evocative names and described in the narrative terms of a situation comedy or soap opera. But these evocations do no more than obscure the evanescence of the lifestyle. One can change one's lifestyle just as O'Connor's airline passenger changes altitude—without being aware of it.

Weiss makes this clear in his popular book *The Clustering of America*. For example, he characterizes the group "Blue Blood Estates" as people who subscribe to *Barron*'s at 9.44 times the average for the nation as a whole, who buy Jaguars at 17.58 times that rate, who drink bottled water at 2.54 times that rate, and so on (1988:271). All of these features are merely contingent elements of those neighborhoods. Doubtless the consumption patterns in Blue Blood Estates change rapidly, as do the residents. But it is almost certain that a newcomer who evinced every single one of those behaviors could move into the neighborhood, yet not be accepted. The way this may occur is critically missing from the geodemographic representation of groups. In fact, there seems little in geodemographics that would enable us to say of a group, viewed at two different times, that it is the *same* group. If Blue Blood Estates is defined in terms of a set of characteristics, as a kind of lifestyle or stereotype, is there any guarantee that *any* of the people who belong to it today will belong to it tomorrow? May one not move in and out of such a group without knowing it? Indeed, it is easy to imagine a situation in which all of the members of a particular group "moved on," replaced by others as they themselves migrated to some other or even new group. At the same time, the groups themselves are subject to change, and such changes can occur for a wide range of reasons. This fluidity, the contingency of relationships among characteristics that define geodemographic groups, the contingency of membership in the groups, and the contingency of the groups themselves, points to the real problem that they pose—they look very much like traditional means for dividing individuals and characterizing groups, but in the end, they are fundamentally different from the means that people use in their everyday lives. There group membership and individual identity are inextricably connected with memory and history and with the belief in the continuity of the elements that make up the social world. To use a geodemographic model as a replacement for more traditional means of characterizing cultures is to dismiss those features—memory, history, and continuity—that have been the very bases for the institutionalization of cultures.

In the same way, there is something missing from the geodemographic representation of places. Here, and as in the case of communities or groups, the relationship between the individual and the place or neighborhood is represented as

one that is strictly contingent. Put the other way around, a place is a concatenation of individuals, connected through a set of contingent relationships. The place itself is simply a spatial location that has attached to it such a set of individuals. But as the geographical literature has long made clear, the relationship between people and places is far richer and more complex than that. People construct the places in which they live in a wide range of ways—by developing rituals and customs, by telling stories, by attaching names and symbols and categorizations to them (Curry 1996b; Tuan 1977). As with social groups, the relationships between people and the places in which they live are often strong and enduring; as David Lowenthal has noted, in the Crusades, people died of nostalgia, of homesickness (1985).

More to the point here, both social groups and places are themselves fundamentally normative. That is, within a group or place, certain things are seen as acceptable, others are not. Indeed, the very practices and attitudes that define a place, far from being neutral criteria, are themselves normative; the features that people see as defining a place tell us both what is seen as right and wrong there and what is seen as characteristic of the place itself. To do certain things is to be seen as a bad neighbor; to do others is to be no neighbor at all. Any group or place has as a part of those defining elements a sense of what is counted as private, of what sorts of behaviors are seen as violations of those standards and of what sorts render one beyond the pale. Indeed, the practices that define the private and the public can best be seen as elements in the spiritual and moral development of both individual and group. Privacy, that is, is fundamental to the functioning of society (Reiman 1984; Wasserstrom 1984; Rachels 1985; Gerstein 1984; Gavison 1983).[9] To fail to see this is to risk being led, once again, down the path of Lotus MarketPlace™.

The Challenge of the Virtual Individual

But if the geodemographic form of geographic information systems represents society in an emaciated way, it represents the individual in a way that is complex and contradictory. As it creates data profiles, it constructs a world of virtual individuals or digital puppets (to use two common names for them), and they raise serious problems for the maintenance of a right to privacy. Indeed, the various calls for controls on data matching were, in an important sense, attempts to protect the individual from government by institutionalizing that fragmentation; the fragmented individual, it was argued, was safer from government control, safer from the Panopticon.

Now, if we turn to current versions of geodemographics, we see, in one sense, images that suggest that individual identity is unitary. For example, in Polk Direct's Niches™, we see the typical "Working Hard" (average income under $20,000; average age 49) described in the following way:

> My late husband Jerry and I used to kick ourselves all the time for not going to college. Oh, I'm doing alright [sic], but it's hard. I really have to work a lot just to stay on my feet. . . . Anyway, even though I work a lot, I do take my share of cigarette breaks. My mom used to smoke too, but what she can't understand is all the health foods I buy. What can I say? One thing my mom can understand though, is the fact we buy only American cars (Polk Direct n.d.).

Here the appeal to narrative conveys a more vivid sense of the individual as one who has a unified identity, where the parts are intrinsically interconnected.

An obvious complaint here, one mentioned above, is that when decisions are made on the basis of these data profiles—themselves constructs of "real" facts about my past purchasing habits, as well as inferences drawn from aggregate data—I am being treated not like "me" but like a caricature. In the image of the 1960s–1970s, I am being treated like a number, a category, a class. There is something to be said for this argument. After all, when the content of both news and advertising available to me is first filtered through a set of suppositions about what I "really want" as a member of some group, in an important sense, I have lost control of my life, and am no longer able to make free and informed decisions.

Recent geodemographic systems, such as Trans Union's Income Estimator (TIE), attempt to remedy at least a portion of this problem by moving to the level of the individual. According to Trans Union:

> TIE does not rely on household income data. TIE does not assume that people earn the same income as their neighbors. . . . TIE is calculated from individuals' previous and current behavior. This objective information is gathered from Trans Union's

> national database, covering the spending and payment behavior of more than 160 million consumers. . . . TIE examines 23 behavioral characteristics identified as most predictive in establishing individual income (Trans Union 1994).

Many people would probably say that Trans Union's claim, that their databases are much more accurate than those of other companies, does little to assuage their fears of a loss of privacy. Most, indeed, would very likely have the opposite reaction, that this simply makes them more worried. But I would suggest that the recent move in geodemographics to more and more individualized profiles offers a means for dealing with the privacy concerns raised by these systems.

I have said above that we might think of the products created by data profiling as "digital individuals." So when I apply for credit, the bank officer "sees" a digital individual; when a credit card company asks Trans Union for a list of prospects, it gets a list of digital individuals; and when the local pizza company sends out a mailing, it sends it not to me, but to a digital individual, one who shares my name and address. There has been a tendency to see these digital individuals as mere "puppets," as images lacking the reality that the "real me" has. But to see them in this way is to be seriously misled. After all, it is today quite common to see individuals as having fragmented personalities. This notion, implicit in criticisms of data matching, is also the cornerstone of Erving Goffman's work (1959, 1981). More recently, other sociologists have made related points (Giddens 1991; Bourdieu 1986), and in the field of computers, Sherry Turkle (1995) has forcefully argued that on the Internet, people live nothing but fragmented lives.

Indeed, I would argue that the solution to a large category of the problems raised by geodemographic systems and by certain versions of geographic information systems and the GIS family is to take digital individuals seriously. We need to see them as important, permanent features of our society and ourselves. Once we begin to understand that these individuals—carrying our names, addresses, and social security numbers—are talking for us, representing us, and making decisions for us, we can see that they are very much like the fragmented parts of ourselves that we present in every part of our everyday life. The digital individual in my credit report is very much like the individual that rents a videotape or deposits a check or rides the bus. It exists in a particular place, but only for a particular purpose. Once it leaves the store or bus or bank, it for all practical purposes ceases to exist. If we take it as obvious that we have control over our actions in the video store or on the bus, we ought too to conclude that as holders of our own identity in a more continuous, physical sense, we should have control over that much wider range of virtual selves, to the creation of which we have been only partially willing collaborators. Here, with Foucault, we need to acknowledge that if it has been traditional to see those in the information industry as selling information about people, it makes more sense to see us as authors of our own lives, of our identities as real and virtual. The information industry acts more as editors and publishers of those virtual identities. And so, just to the extent that geodemographics and geographic information systems create the tools that render those digital individuals more real, they strengthen the case for treating them as real. And if in other ways—in their association with the belief in autonomous technology and their destruction of the principles of fair information practices—they remain a threat to privacy, in this way they offer a solution to the threat to the individual.

If this seems an odd, even eccentric, view, I suggest that it is neither. Indeed, to adopt this view is to link the issue of privacy with that of intellectual property, in the following way. As is well known, there are two main traditions in intellectual property regulation, the Anglo-American labor-based tradition and the Hegelian-based personality theory, or theory of moral right. By contrast, in the theory of moral right, a piece of property is seen as, in a fundamental way, an expression of the personality of the owner; indeed, one becomes fully human only by owning property, just because only in that way can one show the world who one is. This theory of property is not simply a wild fantasy. Personality-based theory was developed not as an attempt to provide a normative basis for property rights, but rather as an attempt to understand how property actually works in a modern society. Further, it is central to European systems of intellectual property; it is formalized in the major international convention on intellectual property, the Berne Convention (Berne Convention 1979), to which the U.S. is a signatory.[10] In the case of works of creativity, this theory has a number of corollaries, among them, that the work is seen as an intrinsic part of its owner and that fundamen-

tal features of the work are permanently attached to the author and cannot be alienated.

Most important, though, is a right closely related to the right of privacy, the right of divulgation; a prospective author cannot be held legally liable for failing to produce a contracted work, since to do so would be to force the author to represent herself in a way of which she did not approve (Curry 1996a, 1996b; Ginsburg 1989; Katz 1951; Hughes 1988; Roeder 1940; Sarraute 1968). So to take the digital individual as real is to offer a conception of the individual that connects the concepts of privacy and intellectual property, while appealing to well-established bodies of theory and well-established institutions. At the same time, because the theory of moral right places the individual fundamentally and intrinsically in the context of the social, it is to move away from the individualist bias that has underlain both the theory and practice of geographic information systems and geodemographics—and that has made it so difficult to understand the problems they raise for privacy.

Notes

1. Here I leave aside a variety of related issues. Of special interest are the issues of intelligent transportation systems and of electronic monitoring of released prisoners, both of which have strong geographic components. For the former, see Agre and Harbs (1994) and Alpert (1994); for the latter, see Corbett and Marx (1991) and Aungles and Cook (1994).
2. My thanks to Rohan Samarajiva for pointing this out.
3. In the analysis of court cases that follows, all of the decisions except *United States v. Penny-Feeney* were written by the U.S. Supreme Court.
4. So in fact we have here a two-part requirement. First, if police have gained evidence from a place that is an "open field," no search warrant is required, because of common law. And second, if the evidence has been gained from a place not an open field, from a home or the curtilage, for example, then the two-fold test laid out in *Katz* comes into play.
5. Although it might be nice if court decisions were so firmly grounded in well-defined conceptional distinctions, a reading of the opinions and dissents in cases associated with search and seizure reveals something rather more unpleasant. One is left with the distinct feeling that the majority decisions have been written with the intent of reaching an end, of getting drug dealers off the streets. One is left with the equally distinct impression that the arguments have been crafted solely with that end in mind, and that appeals to ideas have been used as means of persuasion. Nonetheless, it remains that the courts *have* been able with little dissent to appeal to a very general view of technological change.
6. There is, no doubt, an underlying theory to geodemographics, and that theory surely derives in part from the Chicago School of urban sociology. Nonetheless, the development of geodemographic systems appears itself not to involve anything but the most cursory appeal to such theories.
7. Note that the image of the Panopticon was popularized in Foucault's *Discipline and Punish* (1977), but that Foucault's own argument about the ways in which each person is a party to his or her own surveillance both moves away from Bentham's image and seems particularly appropriate to the case of geodemographics.
8. There have, of course, been more recent claims that maps are not neutral or that they are ineluctably rhetorical (Harley 1988, 1989; Wood 1992). But these claims, to the extent that they are directed against the assumption that people read maps directly, make it clear just how pervasive that realist view is.
9. Here, too, there is a parallel to be drawn with the way neighborhoods or cultures are represented within a geographic information system. This is because of the difficulty in visually representing a culture as other than a concatenation of contingently related traits, and because of the difficulty of expressing values in visual terms.
10. The U.S., whose enacted law of intellectual property is based upon the Anglo-American theory of property, has been able successfully to argue that it incorporates the required moral-right provisions into its legal system because authors who suffer misrepresentation have recourse to the tort system.

Acknowledgments

An earlier version of this article was presented at the Conference on Law and Information Policy for Spatial Databases, sponsored by the Center for the Study of Law, Science, and Technology, Arizona State University College of Law and the National Center for Geographic Information and Analysis, October 28–29, 1994, Phoenix, AZ. This research was supported in part by a grant from the Academic Senate of the University of California, Los Angeles. The author wishes to thank David Flaherty, Gary Marx, and Charles Raab for their comments, and Travis Longcore for research assistance.

Cases Cited

Boyd v. United States, 116 US 616 (1886).
California v. Ciraolo, 476 US 207 (1986).
Dow Chemical Co. v. United States, 476 US 227 (1986).
Florida v. Riley, 488 US 445 (1989).
Hester v. United States, 265 US 57 (1924).
Katz v. United States, 389 US 347 (1967).
Mason v. Montgomery Data, 967 F.2d 135 (5th Cir. 1992).
Olmstead v. United States, 277 US 438 (1928).
Smith v. Maryland, 442 US 735 (1979).
United States v. Karo, 468 US 705 (1984).
United States v. Knotts, 460 US 276 (1983).
United States v. Penny-Feeney, 773 F. Supp. 220 (D. Haw. 1991).
United States v. Place, 462 US 696 (1983).

References

Agre, P., and Harbs, C. A. 1994. Social Choice about Privacy: Intelligent Vehicle-Highway Systems in the United States. *Information Technology and People* 7:63–90.

Alpert, S. 1994. Privacy and Intelligent Highways: Finding the Right of Way. *Santa Clara Computer and High Technology Law Journal* 11:97–118.

Amsterdam, A. G. 1974. Perspectives on the Fourth Amendment. *Minnesota Law Review* 58:349–477.

Aungles, A., and Cook, D. 1994. Information Technology and the Family: Electronic Surveillance and Home Imprisonment. *Information Technology and People* 7:69–80.

Bain, G. D. 1991. Lotus Primes MarketPlace for Desktop Marketing. *MacWEEK* 5:31ff.

Bennett, C. J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Bentham, J. 1791. *Panopticon; or, The Inspection-House: Containing the Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in Which Persons of Any Description Are to be Kept under Inspection: and in Particular to Penitentiary-Houses, Prisons, Houses of Industry, and Schools: with a Plan of Management Adapted to the Principle*. 3 vols. London: T. Payne.

Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886; amended October 2, 1979.

Bourdieu, P. 1986. L'Illusion biographique. *Actes de la recherche en sciences sociales* 62–63:69–72.

Branscomb, A. W. 1994. *Who Owns Information? From Privacy to Public Access*. New York: Basic Books.

Castner, H. W., and Robinson, A. H. 1969. *Dot Area Symbols in Cartography: The Influence of Pattern on Their Perception*. Washington: American Congress of Surveying and Mapping.

Columbia Human Rights Law Review. 1973. *Surveillance, Dataveillance, and Personal Freedoms*. Fair Lawn, NJ: R. E. Burdick.

Commission of the European Communities. 1992a. Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Brussels: European Community.

———. 1992b. Proposal for a Council Directive on the Legal Protection of Databases. Brussels: European Community.

Computer Matching and Privacy Protection Act of 1988. Pub. L. 100-503, Oct. 18, 1988, 102 Stat. 2507.

Corbett, R., and Marx, G. T. 1991. Critique: No Soul in the New Machine: Technofallacies in the Electronic Monitoring Movement. *Justice Quarterly* 8:400–14.

Council of Europe. 1973. Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector. Strasbourg: Council of Europe.

———. 1981a. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe.

———. 1981b. Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg: Council of Europe.

———. 1986: Protection of Personal Data Used for the Purposes of Direct Marketing. Strasbourg: Council of Europe.

Crampton, J. 1993. GIS and Privacy: Crossing the Line? Paper read at Workshop on Geographic Information and Society, Friday Harbor, WA.

Culnan, M. J. 1991. The Lessons of the Lotus MarketPlace: Implications for Consumer Privacy in the 1990s. Paper presented at The First Conference on Computers, Freedom, and Privacy, Burlingame, CA.

Curry, M. R. 1994. Image, Practice, and the Hidden Impacts of Geographic Information Systems. *Progress in Human Geography* 18:441–59.

———. 1996a. Data Protection and Intellectual Property: Information Systems and the Americanization of the New Europe. *Environment and Planning A* 28:891–908.

———. 1996b. *The Work in the World: Geographical Practice and the Written Word.* Minneapolis: University of Minnesota Press.

Dent, B. 1972. Visual Organization and Thematic Map Design. *Annals of the Association of American Geographers* 62:79–93.

Ellul, J. 1964. *The Technological Society*. Trans. John Wilkinson. New York: Random House.

Fishman, C. S. 1988. Technologically Enhanced Visual Surveillance and the Fourth Amendment: Sophistication, Availability, and the Expectation of Privacy. *American Criminal Law Review* 26:315–58.

Flaherty, D. H. 1967. *Privacy in Colonial New England*. Charlottesville, VA: University Press of Virginia.
———. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press.
Flannery, J. J. 1971. The Relative Effectiveness of Some Common Graduated Point Symbols in the Presentation of Quantitative Data. *The Canadian Cartographer* 8:96–109.
Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison*. Trans. Alan Sheridan. New York: Vintage Books.
Friedman, L. M. 1990. *The Republic of Choice: Law, Authority, and Culture.* Cambridge: Harvard University Press.
Gavison, R. 1983. Information Control: Availability and Exclusion. In *Public and Private in Social Life,* ed. S. I. Benn and G. F. Gaus, pp. 113–34. London: Croom Helm.
Gelernter, D. 1992. *Mirror Worlds: Or the Day Software Puts the Universe in a Shoebox: How It Will Happen and What It Will Mean*. New York: Oxford University Press.
Gerstein, R. S. 1984. Intimacy and Privacy. In *Philosophical Dimensions of Privacy: An Anthology*, ed. F. Schoeman, pp. 265–71. Cambridge: Cambridge University Press.
Giddens, A. 1991. *Modernity and Self-Identity: Self and Society in the Late Modern Age.* Stanford, CA: Stanford University Press.
Ginsburg, J. C. 1989. French Copyright Law: A Comparative Overview. *Journal of the Copyright Society of the USA* 4:269–85.
Goffman, E. 1959. *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday Anchor.
———. 1981. *Forms of Talk*. Philadelphia: University of Pennsylvania Press.
Goss, J. 1993. We Know Who You Are and We Know Where You Live: The Instrumental Rationality of Geo-Marketing Information Systems. Paper presented at the Workshop on Geographic Information and Society, Friday Harbor, WA.
———. 1994. Marketing the New Marketing: The Strategic Discourse of Geodemographic Information Systems. In *Ground Truth: The Social Implications of Geographic Information Systems,* ed. J. Pickles, pp. 130–70. New York: Guilford Press.
Granholm, J. M. 1987. Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches. *University of Detroit Law Review* 64:687–713.
Greene, L. H., and Rizzi, S. J. 1997. Database Protection Developments: Proposals Stall in the United States and WIPO. *Journal of Proprietary Rights* 9:2–8.
Gurak, L. J. 1994. The Rhetorical Dynamics of a Community Protest in Cyberspace: The Case of Lotus MarketPlace. PhD dissertation, Rensselaer Polytechnic Institute.
———. 1995. Rhetorical Dynamics of Corporate Communication in Cyberspace: The Protest over Lotus MarketPlace. *IEEE Transactions on Professional Communication* 38:2–10.
Gutterman, M. 1988. A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance. *Syracuse Law Review* 39:647–736.
Harley, J. B. 1988. Silences and Secrecy: The Hidden Agenda of Cartography in Early Modern Europe. *Imago Mundi* 40:57–76.
———. 1989. Deconstructing the Map. *Cartographica* 26:1–20.
Huber, P. 1990. Good Tidings from Lotus Development. *Forbes* 146:136.
Hughes, J. 1988. The Philosophy of Intellectual Property. *Georgetown Law Journal* 77:287–366.
Katz, A. S. 1951. The Doctrine of Moral Rights and American Copyright Law—a Proposal. *Southern California Law Review* 24:375–427.
Lake, R. W. 1993. Planning and Applied Geography: Positivism, Ethics, and Geographic Information Systems. *Progress in Human Geography* 17:404–13.
Larson, E. 1992. *The Naked Consumer: How Our Private Lives become Public Commodities.* New York: Penguin.
Lowenthal, D. 1985. *The Past Is a Foreign Country*. New York: Cambridge University Press.
Marx, G. T., and Reichman, N. 1984. Routinizing the Discovery of Secrets. *American Behavioral Scientist* 27:423–52.
O'Connor, R. J. 1991. Privacy Flap Kills Lotus Database. *San Jose Mercury News*, 1f.
Organisation for Economic Co-operation and Development. 1976. Policy Issues in Data Protection and Privacy. Paris: OECD.
Pickles, J. 1995. *Ground Truth: The Social Implications of Geographic Information Systems.* New York: Guilford Press.
Polk Direct. n.d. Niches from Polk Direct—promotional brochure.
Privacy Act of 1974. Pub. L. 93-579, Dec. 31, 1974, 88 Stat. 1896 (Title 5, Sec. 552a, 552a note).
Rachels, J. 1985. Why Privacy Is Important. In *Ethical Issues in the Use of Computers*, ed. D. G. Johnson and J. W. Snapper, pp. 194–201. Belmont, CA: Wadsworth Publishing.
Reiman, J. H. 1984. Privacy, Intimacy, and Personhood. In *Philosophical Dimensions of Privacy: An Anthology*, ed. F. Schoeman, pp. 300–16. Cambridge: Cambridge University Press.
Robinson, A.; Morrison, J.; Sale, R. D.; and Muehrcke, P. C. 1995. *Elements of Cartography.* 6th ed. New York: John Wiley and Sons.
Roeder, M. A. 1940. The Doctrine of Moral Rights: A Study in the Law of Artists, Authors, and Creators. *Harvard Law Review* 53:554–78.
Rule, J. B. 1973. *Private Lives and Public Surveillance*. London: Allen Lane.

Sarraute, R. 1968. Current Theory on the Moral Right of Authors and Artists under French Law. *The American Journal of Comparative Law* 16:465–86.
Schoeman, F. 1984. Privacy and Intimate Information. In *Philosophical Dimensions of Privacy: An Anthology*, pp. 403–18. Cambridge: Cambridge University Press.
Schwartz, P. 1995. Shock Wave (Anti) Warrior: A Conversation with Alvin Toffler. *Wired* 1:61–65.
Seymour, J. 1991. Lotus MarketPlace Succumbs to Media Hysteria. *PC Week* 8:57.
Simmel, G. 1971 [1903]. The Metropolis and Mental Life. In *Georg Simmel on Individuality and Social Forms,* pp. 324–39. Chicago: University of Chicago Press.
Smith, N. 1992. History and Philosophy of Geography: Real Wars, Theory Wars. *Progress in Human Geography* 16:257–71.
Steele, L. J. 1991. The View from on High: Satellite Remote Sensing Technology and the Fourth Amendment. *High Technology Law Journal* 6:317–34.
———. 1993. Waste Heat and Garbage: The Legalization of Warrantless Infrared Searches. *Criminal Law Bulletin* 29:19–39.
Street, J. 1992. *Politics and Technology*. Basingstoke, U.K.: Macmillan.
Toffler, A. 1970. *Future Shock.* New York: Random House.
Tomkovicz, J. J. 1985. Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province. *Hastings Law Journal* 36:645–738.
Trans Union. 1994. TIE—Trans Union's Income Estimator—Focusing on Your True Target—the Individual.
Tuan, Y.-F. 1977. *Space and Place: The Perspective of Experience*. Minneapolis: University of Minnesota Press.
Turkle, S. 1995. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and Schuster.
Video Privacy Act of 1988. Pub. L. 100-618, Nov. 5, 1988, 102 Stat. 3195.
Voegelin, E. 1940. The Growth of the Race Idea. *The Review of Politics* 2:283–317.
Warren, S., and Brandeis, L. D. 1890. The Right of Privacy. *Harvard Law Review* 4:193–220.
Wasserstrom, R. A. 1984. Privacy: Some Arguments and Assumptions. In *Philosophical Dimensions of Privacy: An Anthology*, ed. F. Schoeman, pp. 317–32. Cambridge: Cambridge University Press.
Weiss, M. J. 1988. *The Clustering of America*. New York: Harper and Row.
Westin, A. F. 1972. *Databanks in a Free Society: Computers, Record-Keeping, and Privacy.* New York: Quadrangle Books.
Winner, L. 1977. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought.* Cambridge: MIT Press.
Wirth, L. 1938. Urbanism as a Way of Life. *American Journal of Sociology* 44:1–24.
———. 1969. Rural-Urban Differences. In *Classic Essays in the Culture of Cities*, ed. R. Sennett, pp. 165–69. New York: Appleton-Century-Crofts.
Wolf, D. B. 1992. Is There Copyright Protection for Maps after Feist? *Journal of the Copyright Society of the USA* 39:224–42.
———. 1993. New Landscape in the Copyright Protection for Maps: Mason v. Montgomery Data, Inc. *Journal of the Copyright Society of the USA* 40:401–06.
Wood, D. 1992. *The Power of Maps*. New York: Guilford.

Correspondence: Department of Geography, University of California, Los Angeles 90095; email curry@geog.ucla.edu.