55
Rethinking privacy in a geocoded world

M R CURRY

GIS are playing a role in undermining privacy. This chapter summarises the concept of privacy, how it has changed over time, and how it has been historically influenced by the introduction of new technologies. It is shown that the ways in which technological developments are regarded as autonomous and the increasing use of the law to define the nature of privacy have eroded traditional safeguards. The growth in use of geographically detailed data has led to the growth of geodemographics and the construction of fictitious personae which are now widely used for direct marketing. These digital personae are reality as far as many commercial and even government processes are concerned. Specifically, the author argues that the trend towards geocoding more and more information will lead to a world without privacy – or with a radically different form of privacy – and urges the GIS community to act responsibly to avert such an out-turn.

1 PRIVACY AS AN ISSUE

Today privacy is a difficult and contentious issue. In the USA the very belief in a constitutionally mandated right to privacy is controversial, seen by some as a litmus test to be applied to potential justices and politicians. And if some wonder whether people have in fact been guaranteed a right to privacy, others claim simply that privacy is dead, killed by a computer technology that has created a world in which, increasingly, everything is open to view.

Given the angry and even apocalyptic tenor of this discourse, it is sometimes difficult to see clearly what is happening. Should there be a right to privacy? Can there be? Yet confusing as it is, this is an issue that ought to be faced, and especially by those who develop and use GIS. These systems and their associated technologies – global positioning systems, remote surveillance systems, and computer cartography – are tied to the very practices and institutions of data collection and surveillance that have figured so prominently in the jeremiads for privacy.

In what follows it will be suggested that the advocates of a right to privacy have made an important point. Indeed, the evidence shows that privacy, far from being a luxury, is a necessity for many of those elements of everyday life – including democracy and science – that we take as valuable. At the same time, the development first of information systems and now of GIS, in concert with other geographical and social changes, has not destroyed that right, but rather resulted in its reconfiguration. If in the past the right to privacy could be seen as a right to be left alone, today it needs to be seen, instead, as a matter of the right of control over one's identity. Those who develop and use GIS, at least to the extent that they believe in things like democracy and science, need to be careful about what they do. And indeed, simply being careful is not likely to be enough.

First, development of the explicit right to privacy over the last 100 years will be described briefly, and in doing so the ways in which the right has been redefined in response to technological changes will be shown. Second, more recent developments will be examined. The computer, in particular, has led to a rethinking of the right to privacy; where before to have a right to privacy was to have a right to be left alone, the development of computerised information

systems means that privacy is now a matter of the protection of data about oneself. Before, one worried about people peeping in one's window; after the development of the computer, one worries about someone peeping into one's past.

Finally, it will be shown that recent developments, largely fuelled by the easy availability of geographical data, have led to a new way of thinking about privacy. With geographically-coded data it is possible to develop profiles of individuals and neighbourhoods, profiles that suppose what people might be like (see Birkin et al, Chapter 51). Thus it is now easily possible to construct around the name of a person, group, or place a new image – an identity that is in one sense fictional, yet that at the same time appears as real as any other. And this geographically-driven development of data profiles has led to a very real need to rethink the right to privacy. Today the desire for privacy is no longer driven by a desire to be left alone. Rather, it is driven by a desire to have control over those multiple identities – identities lodged in direct marketing agencies, credit reports, geodemographic profiles, and the like.

2 THE GENESIS OF THE RIGHT TO PRIVACY

Although privacy itself is old indeed, the formal codification of a right to privacy is rather new. Granted, there has always – at least in the West – existed a strong expectation of something that we would call privacy. But it was codified only in pieces; in the United States Constitution, for example, the closest to an explicit right is the Fourth Amendment, concerning searches and seizures, which 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'.

Through the 19th century, the right to privacy was woven into the pattern of everyday life. In the smallest village there were places where one did not go, things that one did not do or say – at least in public. The strictures against saying the unsayable were seldom stated as formal rules, but rather were enforced through admonition and example. In a small-scale society in which patterns of authority were well established, it was possible for individuals to maintain something that most of us would identify as privacy, even in the absence of a formal codification of its nature.

But in the same century the development both of an increasingly urbanised society and of technological means for the dissemination of information undercut those patterns of authority. As Georg Simmel bemoaned in his famous 'The metropolis and mental life' ([1903] 1971) and Louis Wirth later formalised for American urban sociology (Wirth 1938, 1969), the urban became a place in which an individual could choose to remain isolated and anonymous.

And so, toward the end of the 19th century a formal right to privacy was first described in the USA, in a famous law-review article by Warren and Brandeis (1890). There they claimed that technological changes, such as the newspaper, allowed an anonymous writer to make claims about individuals, without having to face those individuals. We needed a right to privacy to ensure our ability 'to be left alone'. So the problem for privacy created in this new landscape, where the actions of the individual seemed much less constrained by custom, was solved by the development of a formalised set of privacy guarantees.

In the end – and this should be no surprise, given that privacy has evolved as a set of everyday practices and institutions – this turned out not to be a simple task. Indeed, the Flaherty (1989) catalogue of the elements of the right to privacy shows it to be extraordinarily complex:

- the right to individual autonomy;
- the right to be left alone;
- the right to a private life;
- the right to control information about oneself;
- the right to limit accessibility;
- the right of exclusive control of access to private realms;
- the right to minimise intrusiveness;
- the right to expect confidentiality;
- the right to enjoy solitude;
- the right to enjoy intimacy;
- the right to enjoy anonymity;
- the right to enjoy reserve;
- the right to secrecy.

The right to privacy developed within larger communities, but central to that right has long been the view that the home is the central locus of private

activities, the place where one really can be left alone. Or to be more exact, in keeping with common law, what is important has been less that area bounded by four walls than the somewhat larger area within which the intimate activities of everyday life were taking place; this 'curtilage' consisted of (as the Oxford English Dictionary puts 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.'

Indeed, in the USA the courts long recognised that the distinction between the dwelling-house and curtilage, and the 'open fields' beyond is 'as old as the common law' (Hester v. United States 1924: 59).

Yet by the 1920s the telephone had begun to undercut the distinction between the home and curtilage and that which lay beyond. This change was quickly reflected in court cases. In 1928, in Olmstead v. United States, the Supreme Court 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 [Fourth] Amendment can not 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 . . .' (Olmstead v. United States 1928: 465–6).

In their view, a wiretap involved no invasion of privacy, since it did not involve: '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).

In the USA this was for many years the guiding legal view; the possibility that technological change required a rethinking of the nature of privacy was simply rejected. But by the 1960s the weight of technological change had increased to the point at which it became much easier to engage in just such a rethinking. Indeed, it seems fair to believe that since that time the nature of privacy has been constantly at issue.

For example, in the late 1960s, in Katz v. United States (1967), the Supreme Court for the first time asserted that modern urban life calls for a rethinking of the 'age-old' distinction between the home and the public beyond. Recognising that the telephone is a medium for private conversations, and that people often engage in telephone conversations while away from home, the Court concluded 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. In effect the Court recognised that the modern, technologically connected city is a new sort of landscape.

This reforming of the modern urban-industrial landscape, prefigured in Warren and Brandeis but not really acknowledged until much later, was central to the rethinking of privacy through the 1960s. But a second factor has been equally important, and that is the development of the computer.

If the computer has only really become ubiquitous in the last 15 years, there have nonetheless been two moments in which some believed it possible to see the direction in which information processing equipment was pointing. The first was in the era between the 1910s and the 1930s. Then, as Beniger (1986) has pointed out, information processing equipment previously used for purely technical purposes began to be used to 'strengthen the control maintained by the entire bureaucratic structure' (Beniger 1986: 408). Symbolically, this era was captured by the production of America's first Social Security retirement payouts, in 1937, on a punched card. And indeed, as Beniger notes, the arrival of the punched card was greeted in some quarters by a fear that the new system depersonalised people, turning them into mere numbers.

More familiarly, the second moment occurred in the 1960s. At that point, the arrival in government offices of mainframe computers and magnetic tape storage seemed to many to signal an escalation in government's ability to maintain stores of information about its citizens. And for a number of reasons – certainly including the political climate surrounding the Vietnam War and the civil rights movement – there was in this era a public outcry against the possibility of governments creating large databanks of information on individuals and groups (Columbia Human Rights Law Review 1973; Mowshowitz 1976; Rule 1973; Westin 1972).

Central to privacy concerns was the belief that by using computers, governments would be able to combine individual databases into systems that contained comprehensive, cradle-to-grave dossiers on every citizen and resident. If totalitarian countries had previously managed this task using paper records, the ability to create computerised dossiers that could easily be communicated seemed to many to be far more troubling.

In response to political pressure, it was during this era that a number of countries developed systems for the control of these data. In the USA, the issue was hotly debated. Relying in part on the recommendations of a Senate committee (US Senate 1974), Congress passed the Privacy Act (US 1974). At the same time, and relying to varying degrees on proposals developed by the Organisation for Economic Cooperation and Development (OECD 1976), the Commission of the European Communities (1980), and the Council of Europe (1981a), most of the countries of Western Europe passed similar legislation (Bennett 1992; Flaherty 1989).

One feature that the laws enacted in the USA and Europe had in common was a belief that the primary source of threats to individual privacy was government. And the focus of concern, by and large, was the possibility that standard identifiers, such as the US Social Security Number, might be used in a process called 'data matching' to combine dossiers across agencies.

There were, it needs to be granted, privacy concerns directed at non-public bodies. In Europe there has been widespread concern for over 20 years, evinced in documents emerging from the Council of Europe (Council of Europe 1973, 1981a, 1981b, 1984, 1986, 1989, 1990), the European Commission (Commission of the European Communities 1980, 1991), and the Organisation for Economic Cooperation and Development (OECD 1976, 1992). But in the USA, and to a lesser degree in Europe, the fact that such non-public bodies were seen as constituting less of a threat is indicated by the piecemeal approach taken to them. At the extreme, in the USA privacy issues in the private sector have been taken up as they moved into public consciousness, as when the inquiry by reporters into the video-rental records of a nominee to the Supreme Court motivated members of Congress to pass the Video Privacy Act (US 1988).

As Bennett (1992) has noted, one of the striking things about privacy regulations in Europe and America has been their similarity. Although the means for protection have varied, the regulations have in common an appeal to what have come to be known as the fair information principles. These require that any body which maintains a system containing information about individuals must:

- make public the existence of the system;
- give individuals access to data about them;
- give individuals the right to correct erroneous information.

Furthermore,

- personal data should be collected only where necessary;
- personal data should be used only for the purposes for which they were collected;
- personal data should not to be disclosed to another group or agency without some sort of consent;
- personal data should be securely stored.

And so, if through the 19th century privacy was conceived as a matter of the establishment of an appropriate arena within which people could be left alone, the joint development of an industrial, urban society and of the computer had, by 100 years later, led to a refiguration of the concept. The central concern by the 1970s was to protect the data that had been collected by government organisations. The fair information principles laid out what seemed to be appropriate means for the achievement of that goal.

3 THE COMING OF GIS

During the period of the first real flowering of the computer, in the 1960s, concerns about privacy typically centred around the belief that by using a computer some centralised authority – typically a government – would be able to gather large amounts of information about individuals. Indeed, almost every government database relied in the end on the attaching of an identifying number (such as the American Social Security Number or the Canadian Social Insurance Number) to each individual.

But whatever the problems with such systems, they have one merit: the data are only collected about individuals – which was the focus of the fair information principles. With the right set of rules and procedures it would be possible for each

individual to check the accuracy of a dossier, making corrections where needed.

It is here that the coming of the geocoded world dramatically recasts the problem of privacy regulation, and then the nature of privacy itself. There are, in fact, two rather separate moments to this refiguration. First, there are changes in the nature and availability of data about individuals, households, and groups. These changes are having a direct effect on the nature of everyday life, both by reshaping those elements of life that have in the past been called 'private' and by creating new elements from which will be constructed a new way of thinking about the private realm. And second, there are certain features of these technological developments that make them seem natural and normal. As a consequence, the accompanying changes in the nature of the right to privacy are, to a degree, seen as equally natural and normal. Putting the matter simply, there are two issues related to the advent of widespread use of GIS: the ways in which privacy is changing and the ways in which those changes are being greeted.

3.1 GIS and the changing nature of privacy

It seems likely that those involved in the development of the GBF-DIME files in the US Bureau of the Census and in the development of the zone improvement plan (ZIP) code in the US Postal Service had no real conception of the future impact of those developments. The GBF-DIME files, after all, were developed primarily as an aid to the streamlining of the decennial census, just as the ZIP code was a way of streamlining the sorting of mail. Yet in the end, the two combined into a branch of GIS that has been deeply connected with the refiguration of private life, and hence with a need to rethink the nature of the right to privacy. This branch is geodemographics.

The development of a computerised system to map the areas occupied by most Americans was a major step toward a refiguration of the right to privacy. This was even more the case because of the ways in which that mapping occurred; in the end it became possible to associate street names and address ranges with geographical coordinates, and so through interpolation geographically to locate the address of any household in urban (and later all) America. Subsequently, much more precise geographical coordinates have been introduced in other nations, notably in Britain.

The general introduction in the late 1960s of the postal ZIP code in America preceded slightly the Census Bureau's computer mapping system. Nonetheless, the ZIP code – the second arm of the geodemographic revolution – was immediately seized upon by the marketing industry. For example, in a 1967 article 'Zip Code – New Tool for Marketers', Baier hailed it as 'a "built-in" and universal means of geographical identification' (Baier 1967: 140). As he put it: '[The] ZIP Code System offers a new, unique opportunity; the way it has been put together (although devised for quite a different reason, namely postal efficiency) just happens to fit many marketing needs' (Baier 1967: 136).

And with the development of computer mapping systems, marketers, and others, were now able to combine data from the Census Bureau's mapping project with data from the Postal Services Carrier Route Information System (which consisted of a comprehensive listing of mailing addresses) and therefore to create lists that provided a geographical location for every address in the nation. Thus was born the geocoded society.

From the point of view of the issue of privacy, two aspects of this technological development were of immediate importance. First, it meant that the locus of information moved from the individual to the household. And second, marketers immediately noted that the new system allowed them a much more powerful way of applying an insight that they had long had, that 'people with like interests tend to cluster' (Baier 1967: 136).

By the early 1970s the first of a growing group of corporations were established with the aim of applying this insight – that people tend to cluster with others of like characteristics – in the context of increasingly powerful and affordable computer technology. These companies, engaging in what they termed 'geodemographics', moved rapidly away from the mere collection of information about individuals (Curry 1992, 1997; Goss 1995; Larson 1992; Weiss 1988). Faced with restrictions (such as the American Fair Credit Reporting Act of 1970: US 1970) on the collection of individual information, they began to take the household as the primary unit. At the same time, relying on the theory that people cluster with others like themselves, they began to develop methods of 'data profiling'.

In data profiling the aim is not to say what an individual or household is like. Rather, it is to say what that individual or household is *probably* like.

Drawing upon a wide array of government data, market surveys, and purchasing records, producers of geodemographic profiles divide an area into a small number of regional types and then attribute the characteristics of that type to each household (see Birkin et al, Chapter 51). If household or individual data are available, those data may be added to enhance the discrimination capability and guide automated decisions made about which household is to receive which piece of advertising, which version of a news magazine, which offer of credit.

It is this profiling which undercuts traditional methods for the protection of the right to privacy and at the same time results in a refiguration of that right. For if it seemed possible, at least in theory, to apply the fair information principles to individual data, just how that might be done in the case of geodemographic data is not at all clear. Geodemographics creates a whole new range of individuals – what has been called 'digital individuals' (Agre 1994) or the 'digital personae' (Clarke 1994) – and households. If in the past everyone had a reputation, these reputations are now codified, stored in computers, and bought and sold. Through geocoding we now have a world of virtual households and virtual selves, taken by many people to be more real than old-fashioned physical ones.

All this indicates that the nature of privacy itself needs to be rethought as it was 100 years ago. For if the traditional functions of privacy are to persist, that is to allow people to control what aspects of themselves can be seen, to allow them to develop their personalities, to allow the testing of ideas that is essential to democracy, to science, and to economic innovation, what counts as privacy needs to change. People need to have control over the virtual individuals and virtual selves that others create.

4 IMPEDIMENTS TO A NEW RIGHT TO PRIVACY

There are two impediments to the sort of rethinking of privacy suggested above. Both, as it happens, are directly concerned with issues raised not simply by geodemographics, but rather by GIS more generally.

The first of these impediments is a very general way of thinking about technology and social change. It will be useful here to turn away from GIS to one of the predecessors of these systems, the paper map. The paper map has two striking features. Just to the extent that it includes identifiable elements it appears to contain the possibility of being linked with other maps, and indeed, with all other maps. It seems possible, in principle, to create one very large map that is a compendium of all other maps. Here, in fact, the map – just because of the way in which it points to the face of the Earth – appears to provide just the model of the organisation of knowledge that has eluded those who have attempted to organise discursive knowledge.

At the same time, when we see an object or event located on a map it seems perfectly possible to locate that event with increasing accuracy. If we had a map constructed at a one-to-one scale, we could quite literally show exactly where I am sitting as I write this, down to the smallest fraction of a millimetre.

In these two ways, by seeming intrinsically to allow for the concatenation of maps and by seeming intrinsically to involve a concept of absolute accuracy, the map appeals to and seems to support the idea that the development of the map is preordained. That is, the map seems to support the view that left unfettered, maps would come to be more and more accurate, and more and more interconnected. The map seems to support the notion that the development of technologies is, as Langdon Winner has termed it, 'autonomous' (Winner 1977).

As appealing as this idea is, and it has a long history of support, there is little to justify it. Indeed, Mackenzie (1990) has shown in the similar case of missile guidance systems just how little this view of accuracy can be justified. But justified or not, the view of the map – and now the GIS – as developing autonomously has worked its way both into popular culture and into common sense. And there, true or not, it has an effect on the understanding of privacy. To the extent that people believe the development of privacy-related technologies to be an inexorable process with a preordained goal, they are likely to see that process as natural and normal, and are likely to see the right to privacy as something that must undergo a regular process of diminution. Indeed, this is the very understanding of the right to privacy that has over the last 20 years been enunciated in the US courts (Curry 1997a). So even ignoring geodemographics, the very existence of the family of technologies that make up GIS – and especially remote surveillance systems and global positioning systems – has an impact on the right to privacy.

There is a second impediment to the reconceptualisation of privacy as an associated right. It was suggested earlier that in the USA the right to privacy as a formal right was articulated about 100 years ago. A critical feature of that articulation, and one that was not mentioned, was that in the famous Warren and Brandeis law review article they not only defined a right to privacy, but defined that right as a legal right. Before that time, privacy had been something that people had by virtue of being in particular places and social situations; the violation of privacy was therefore a social violation. But after Warren and Brandeis, and more so after Griswold v. Connecticut (1965), privacy became a legal right.

In fact, a fundamental impediment to the rethinking of privacy is the extent to which the discourse around privacy has come to be seen in the first instance as a legal discourse. And here too, though in a less obvious way, the development of GIS can be seen as supportive of the increased hegemony of legal discourse (see Onsrud, Chapter 46), and the accompanying decline of other forms of moral and social discourse, and control. As noted elsewhere (Curry 1994, 1995, 1996), an important feature of GIS has been their role in recasting traditional systems of ownership and authority. The creator of works in science could at one time expect to obtain ownership rights in those works, where those rights were in a fundamental way outside the legal system. Newton, to take an obvious example, did not need to hire a lawyer in order to get credit for his laws. The credit was given within the context of a system that defined that credit in social and moral terms.

But GIS, like the rest of big science (Pickering 1989; Price 1963), move us away from the traditional model of the scientist as heroic loner, to the new model of the institutionally and technologically GIS-supported research manager, allocating rights and responsibilities in detailed and formalised ways. And to the extent that a scientist is using hardware, software, and data of the complexity of those involved in the typical GIS, he or she is embracing a move from social means of guaranteeing appropriate behaviour to legal means. The upshot of the use of the systems in geography, as elsewhere in science, is a social system in which rights and responsibilities are allocated through that legal system; it is a system that sees the problems of human interaction as definable in strictly legal terms.

5 RETHINKING THE NATURE OF PRIVACY

It may now seem as though I have painted a bleak picture. We are moving toward a geocoded society, a society in which for every physical self there are a dozen or more 'virtual selves', applying for credit, buying magazines, renting apartments, looking for the perfect spouse. These selves, constructed from bits and pieces of data, much of it associated with me only because of where I live, work, or shop, are taken by many people to be more real than the real one. And in an important sense these selves are not only beyond my control, they are beyond the control of anyone – at least if we rely on the fair information principles. For those principles were developed for a world without geocoding.

Yet as far as the rethinking of the nature of privacy is concerned, one has to say on the evidence that it *is* occurring. One need not look just at academic articles in order to find a wide-ranging dissatisfaction with current ways of thinking about the issue. Certainly this was expressed several years ago in the Lotus MarketPlace dispute (Bain 1991; Culnan 1991; Gurak 1995; Seymour 1991). When Lotus announced a software/data product that would work on a desktop computer and would provide to small business the same detailed geodemographic and personal information about most of the households in the country that had long been available to large data users, there was a widespread and vigorous response. In the end, having received more than 30 000 requests to have individual information deleted, Lotus decided not to introduce the product.

A similar response greeted the 1996 rumour – that Lexis-Nexis would introduce a system called 'P-Trak', that would consist of records containing individuals' social security numbers and the maiden names of their mothers (a common security identifier). Although Lexis-Nexis denied that there was ever a plan to contain highly personal data in the system, they did back down, and removed social security numbers (Aguilar 1996; Flynn 1996a, 1996b). In both cases the public complained not about the existence in these databases of confidential or inaccurate data, but rather about the release of those data in ways that constituted uncontrolled, digital identities.

So whatever the impediments to the rethinking of the nature of privacy, it appears that that rethinking is in fact occurring, although not always in the name

of privacy. But this leaves the second question: if people are now rethinking the ways in which they wish information about themselves to be available, if they are rejecting the wholesale proliferation of virtual selves, how ought these changes be reflected in the work of the everyday user of a GIS?

The first and most obvious answer – that the creator and the user of a GIS ought to be careful and ought not to produce works that will patently be damaging – is both an inadequate one and a truism. It needs to be said, though, simply because in the current frenzy of data buying and selling and in the current political climate there are many who would take the position of Lexis-Nexis, who responded to the P-Trak controversy by saying the company could not be held responsible for what is done with the service's information (Aguilar 1996). Yet to be careful is not enough, as the history of the right to privacy that I have sketched above shows; surely none of the inventors or early promoters of the telephone or the computer could have predicted its impacts.

A second step, and a step in the right direction, would be to recognise that new technologies can make old laws obsolete. Nowhere is this more true than in the case of public records. For public records, such as property assessments and court documents, were made public in a time in which getting those records was recognised to be not easy. It required going to the appropriate office in the appropriate city at the appropriate time, waiting in line, laboriously copying materials by hand and sometimes giving a well-placed gift.

Once placed on computers, those same records can easily be accessed by a person with a modem and a little free time. Where before few would have bothered to look at their neighbours' property assessments, now many more can and with much greater ease. Rules for access that under one set of technological conditions meant one thing now mean something very different.

Even this recognition – and an accompanying action – may well leave the user of GIS in the position of unwittingly supporting a means of undercutting the right to privacy. One solution here, and one that has some support in Europe, would simply outlaw the mixing of data pertaining to aggregations with individual data; it would assume that, in the mixing, the data become personal and hence it would make illegal much of what is now the direct marketing business.

This tack has the advantage that it appeals to an existing, and even common, model of a privacy-friendly way of thinking about individuals and households. That is the model that we use in thinking about our relations with our own work and the relations of other people to theirs. It is a model that abjures the traditional American and British conception of ownership, and instead operates in terms of a European conception. This European conception, often termed the 'personality' or 'moral-right' model, has long been used, and is in fact incorporated into national and international copyright agreements (see, for instance, Grelot 1997). It specifies that individuals have the right to control the ways in which that which they make can be used and modified, just because the products that individuals create are intrinsic to their identities. As scientists we routinely appeal to this very system; it is, after all, the one that we are taught in graduate school. And it is one that in important ways serves us well.

We would do well, in our work, however, to recognise this fact and, where possible, take it to heart, yet it seems extraordinarily unlikely that such an approach will be formally recognised in the USA. Indeed, and as I have suggested elsewhere, the USA is involved not in adopting such a view but rather in promoting its abolition in those places, primarily in western Europe, where it is now held (Curry 1996). And recent initiatives, such as the World Intellectual Property Organisation's (1996) 'Draft Treaty on Intellectual Property in Respect of Databases', appear in the law to signal the end of the moral-right view and with it the demise of the traditional means of regulating the exchange of scientific data.

There are ways though in which one can create a GIS that does not fit so easily into systems that undercut personal privacy. One major way in which the systems contribute to a diminution in personal privacy arises from their use of geocoding. But paradoxical as it sounds, one can in fact create GIS that do not use geocoding; and such systems, to the extent that they are much more difficult to combine with others, offer a degree of protection. So geographers ought – if they are serious about privacy – also to take seriously the need to question the ways in which they carry out their work. In particular, they need to question the belief that, where geocoding is possible, it ought to be done. In the end, a world in which everything is geocoded will be a world in which virtual individuals and households are everywhere and in which they cannot be controlled. It will be a world without privacy.

References

Agre P E 1994 Understanding the digital individual. *The Information Society* 10: 73–6

Aguilar R 1996 Service pulls Social Security numbers. *C/Net* June 12 1996

Baier M 1967 Zip code – new tool for marketers. *Harvard Business Review* 45: 136–40

Bain G D 1991 Lotus primes MarketPlace for desktop marketing. *MacWEEK* 5: 31ff

Beniger J R 1986 *The control revolution: technological and economic origins of the information society*. Cambridge (USA), Harvard University Press

Bennett C J 1992 *Regulating privacy: data protection and public policy in Europe and the United States*. Ithaca, Cornell University Press

Clarke R 1994 The digital persona and its application to data surveillance. *The Information Society* 10: 77–94

Columbia Human Rights Law Review 1973 *Surveillance, dataveillance and personal freedoms*. Fair Lawn, R E Burdick

Commission of the European Communities 1980 *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security*. Brussels, European Community

Commission of the European Communities 1991 *Opinion on the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*. Brussels, European Community

Council of Europe 1973 *Protection of the privacy of individuals vis-á-vis electronic data banks in the private sector*. Strasbourg, Council of Europe

Council of Europe 198la *Convention for the protection of individuals with regard to automatic processing of personal data*. Strasbourg, Council of Europe

Council of Europe 1981b *Regulations for automated medical data banks*. Strasbourg, Council of Europe

Council of Europe 1984 *Protection of personal data used for scientific research and statistics*. Strasbourg, Council of Europe

Council of Europe 1986 *Protection of personal data used for the purposes of direct marketing*. Strasbourg, Council of Europe

Council of Europe 1989 *Protection of personal data used for employment purposes*. Strasbourg, Council of Europe

Council of Europe 1990 *On the protection of personal data used for payment and other related operations*. Strasbourg, Council of Europe

Culnan M J 1991 The lessons of the Lotus MarketPlace: implications for consumer privacy in the 1990s. Paper read at The First Conference on Computers, Freedom and Privacy

Curry D J 1992 *The new marketing research systems: how to use strategic database information for better marketing decisions*. New York, John Wiley & Sons Inc.

Curry M R 1994 Image practice and the hidden impacts of geographic information systems. *Progress in Human Geography* 18: 441–59

Curry M R 1995b Rethinking rights and responsibilities in geographic information systems: beyond the power of the image. *Cartography and Geographic Information Systems* 22: 58–69

Curry M R 1996 Data protection and intellectual property: information systems and the Americanisation of the new Europe. *Environment and Planning A* 28: 891–908

Curry M R 1997a Geodemographics and the end of the private realm. *Annals, Association of American Geographers* 87: 681–99

Flaherty D H 1989 *Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, The University of North Carolina Press

Flynn L J 1996a Company stops providing access to social security numbers. *New York Times* June 13 1996

Flynn L J 1996b Lexis-Nexis flap prompts push for privacy rights. *New York Times* October 13 Cyber Times Extra

Goss J 1995 'We know who you are and we know where you live' the instrumental rationality of geodemographic information systems. *Economic Geography* 71: 171–98

Grelot J-P 1997 The French approach. In Rhind D W (ed.) *Framework for the world.* Cambridge (UK), GeoInformation International: 226–34

Griswold v. Connecticut. 1965 381 *US 479 (1965)*

Gurak L J 1995 Rhetorical dynamics of corporate communication in cyberspace. The protest over Lotus MarketPlace. *IEEE Transactions on Professional Communication* 38: 2–10

Hester v. United States. 1924 265 *US 57 (1924)*

Katz v. United States. 1967 389 *US 347 (1967)*

Larson E 1992 *The naked consumer: how our private lives become public commodities*. New York, Penguin

Mackenzie D 1990 *Inventing accuracy: an historical sociology of nuclear missile guidance*. Cambridge, MIT Press

Mowshowitz A 1976 *The conquest of will: information processing in human affairs*. Reading (USA), Addison-Wesley

OECD 1976 *Policy issues in data protection and privacy*. Paris, Organisation for Economic Cooperation and Development

OECD 1992 *Privacy and data protection – issues and challenges*. Paris, Organisation for Economic Cooperation and Development

Olmstead v. United States. 1928 277 *US 438 (1928)*

Pickering A 1989 Big science as a form of life. Paper read at 'The restructuring of the physical sciences in Europe and the United States 1945–1960' 19–23 September 1988, Singapore

Price D J de S 1963 *Little science big science*. New York, Columbia University Press

Rule J B 1973 *Private lives and public surveillance*. London, Allen Lane

Seymour J 1991 Lotus' MarketPlace succumbs to media hysteria. *PC Week* 8: 57

Simmel G [1903] 1971 The metropolis and mental life. In *Georg Simmel on individuality and social forms.* Chicago, University of Chicago Press: 324–39

US 1970 Fair Credit Reporting Act of 1970. 15 *USC. Sec. 1681*

US 1974 The Privacy Act of 1974. *PL 93-579 15 USC 552a Sec. 3 (e) (4)*

US 1988 Video Privacy Act of 1988. 18 *USC Sec. 2901*

US Senate Subcommittee on Constitutional Rights of the Committee on the Judiciary 93d Congress 2d session, 1974 *Federal data banks and constitutional rights*. Washington DC, US Government Printing Office

Warren S, Brandeis L D 1890 The right of privacy. *Harvard Law Review* 4: 193–220

Weiss M J 1988 *The clustering of America*. New York, Harper and Row

Weiss M J 1994 *Latitudes and attitudes: an atlas of American tastes, trends, politics, and passions*. Boston, Little, Brown and Co.

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 (USA), MIT Press

Wirth L 1938 Urbanism as a way of life. *American Journal of Sociology* 44: 1–24

Wirth L 1969 Rural-urban differences. In Sennett R (ed.) *Classic essays in the culture of cities.* New York, Appleton-Century-Crofts: 165–9

World Intellectual Property Organisation 1996 *Draft treaty on intellectual property in respect of databases*. Geneva