Geographic Information Technologies and Personal Privacy

Marc P. Armstrong
Department of Geography / The University of Iowa / Iowa City / IA / USA

Amy J. Ruggles
Rand McNally & Co. / Skokie / IL / USA

Abstract

Concepts of privacy are fluid. They change according to historical contingencies and are mediated by technology. Geospatial technologies are now altering the way privacy is being considered. Remote sensing technologies can be used to observe, or infer, the locations of individuals from space, from remotely piloted aircraft, and from fixed terrestrial observation points. Other geospatial technologies can be used to track movements and to recover individual-level information from maps. These changes are welcomed by some, since they provide a certain level of public safety (e.g., E-911). In other cases, however, a lack of awareness about the sinister aspects of surveillance may lead to complacency. Where personal privacy is eroded, individuals should be aware of the limitations of technology and the degree to which it may be applied to monitor their activities.

Keywords: privacy, geocoding, remote sensing, location-based services

Résumé

Le concept de la protection de la vie privée est plutôt vague. Il change avec les contingences historiques et les technologies. De nos jours, les technologies géospatiales modifient la perception que nous avons du respect de la vie privée. Les techniques de télédétection permettent de déterminer ou de déduire l'endroit où se trouvent des personnes à partir de l'espace, d'aéronefs téléguidés et de points d'observation fixes au sol. D'autres technologies géospatiales permettent de suivre les mouvements des gens et de recueillir des renseignements personnels à leur sujet à l'aide de cartes. Si certains voient d'un bon œil ces changements parce qu'ils assurent une certaine protection publique (p. ex., E-911), d'autres croient qu'un manque de conscientisation concernant les aspects néfastes de la surveillance pourrait engendrer un certain laisser-aller. Lorsqu'il est question de vie privée, les gens devraient connaître les limites de la technologie et comment elle est employée pour suivre leurs activités.

Mots clés: vie privée, géocodage, télédétection, commerce mobile

Introduction

Though privacy is often viewed as a basic human right, concepts of privacy are culturally conditioned and continually co-evolve with changes in technology (Dash, Schwartz, and Knowlton 1959; Diffie and Landau 1998). Recent developments in geospatial information technologies have begun to generate rising levels of concern about privacy in the popular media. While researchers have initiated discussion about emerging interactions between geospatial technologies and individual-level privacy (Armstrong, Rushton, and Zimmerman 1999;

Armstrong 2002; Curry 1997, 1998; Dobson 1998, 2000; Dobson and Fisher 2003; Goss 1995; Monmonier 2002; Onsrud, Johnson, and Lopez 1994; Waters 2000), the rapid pace of co-evolutionary change requires further elucidation of emerging issues. The general purpose of this article, therefore, is to sketch out the role, both actual and potential, that geospatial technologies play in the negotiation of personal privacy. Particular emphasis is given to the surveillance capabilities of remote sensing systems (satellite and terrestrial) and to how administrative records and other information, sometimes obtained as an adjunct of newly emerging location-based services, can be mapped and cross-referenced to reveal the identities and characteristics of individuals from information that is often available on-line.

Though writers such as Jeremy Bentham (1843) and Michel Foucault (1977), in their discussions of the panopticon, did not explicitly anticipate panoptic surveillance and the routine use of geospatial technologies to monitor the space–time activities of individuals, many scholars (see Elden 2003; Koskela 2003; Wood 2003) are increasingly concerned about such issues. In the case of remote sensing technologies, this role has already been explicitly acknowledged in the title of one of the first edited books on this topic: *The Surveillant Science: Remote Sensing of the Environment* (Holz 1973). While other geospatial technologies lack such a specific label, they clearly are being used, both individually and in combination, in surveillance. Moreover, as existing technologies develop, becoming smaller, lighter, and faster, and as their prices plummet, they will penetrate into most facets of our daily lives. Many individuals will complacently welcome these new technologies because of their real (or imagined) benefits. In other cases, however, awareness of the power of such technologies will encourage some to attempt to geospatially cloak themselves, living in the shadows of the panopticon.

The Gaze of Remote Sensing Technologies

Remote sensing refers to the process of recording, without direct contact, the electromagnetic radiation that is reflected or emitted from objects. Enormous improvements in the price and performance of imaging, recording, and communication technologies have important implications for both satellite and terrestrial surveillance systems. The following sections briefly consider the progression of increases in resolution of satellite remote sensing systems, then shift attention to what is becoming a ubiquitous network of terrestrial surveillance technologies. Satellites are particularly important because they are effectively unobserved and because they repeatedly (daily, weekly, monthly) image the same location, thus provide the opportunity for change detection.

THE EVOLUTION OF RESOLUTION

The first digital civil remote sensing satellite (initially called Earth Resources Technology Satellite, or ERTS, but later renamed Landsat) became operational in 1972 with a relatively crude ground resolution of approximately 80 m. The resolution of such systems, however, has continued to increase over time (see Jensen 2004), and the latest-generation systems, licensed by the US Department of Commerce (US Department of Commerce 2005), now offer sub-metre resolution (Canada and other countries have their own licensing policies). The Quickbird system, for example, provides imagery with a resolution of 61 cm (see Baker, O'Connell, and Williamson 2001). An additional trend in remote sensing technology is also lending a hand to stealthy high-resolution sensing: remotely piloted aircraft. These drone-like aircraft are designed to remain aloft for long periods, operate quietly, and fly close enough to the ground to capture high-resolution images, which are transmitted to receiving stations for processing and interpretation. Such systems are widely deployed by the military and are now diffusing into the public sector.

To illustrate the implications of advanced remote sensing technologies on individual-level surveillance, it should be noted that wildlife managers have used photographic remote sensing for decades to conduct wildlife censuses. Snow geese are easily detectable (and can be enumerated) when they are swimming or flying over most water bodies because they contrast well with the background. Moreover, at 0.5-m spatial resolution, counting individual humans becomes a more straightforward activity. If individuals come too close together, they can no longer be resolved as individuals, though knowledge about a scene can be used to augment interpretation. For example, the size of a cluster of people can be used to support count estimates, if assumptions are made about personal space in the cultural setting observed (Hall 1959, 1966). Such practices are used by law enforcement and by the press to estimate attendance at outdoor venues such as political demonstrations and concerts.

Even with the possibility of centimetre-accuracy images (which are already available from aircraft platforms), significant checks are in place to prevent remote sensing from intruding completely into everyday lives. First, let us consider the visible and near-infrared portions of the electromagnetic spectrum. In those cases, a simple solution available to all privacy seekers is simply to go indoors. Most satellite sensors are not designed to operate with low look-angles, in part because their purpose is to record map-like images from a (near) vertical perspective. While corrections can be made, atmospheric distortion becomes problematic as the length of atmospheric travel increases. Though limited directional (off-nadir) pointing is already a feature of some satellite systems, it is impossible for a satellite to collect a visible-spectrum image from an indoor target. Even with the look angles provided by low-flying aircraft (piloted or not), roofs provide significant protection from surveillance.

If, however, we move along the electromagnetic spectrum to the thermal infrared (IR) bands, it is *conceptually* possible to collect information about people in dwellings, though practical implementations remain difficult. Thermal IR sensors detect radiation that, unlike reflected electromagnetic radiation, has been absorbed and re-emitted. Because such energy can be distorted by wind (smear), crisp high-resolution images are difficult to obtain if radiation must travel long distances through the atmosphere. High-resolution thermal sensing, however, is eminently practicable from aircraft and terrestrial vantage points and has been widely used in energy audits and to deduce that cannabis cultivation is taking place in residences by sensing the waste heat produced by grow-lamps.[1] In a spy-versus-spy escalation, growers are fighting back by increasing insulation and exhausting waste heat into sewer standpipes. This and other types of terrestrial sensing are clearly an important growth industry, as examined in the next section.

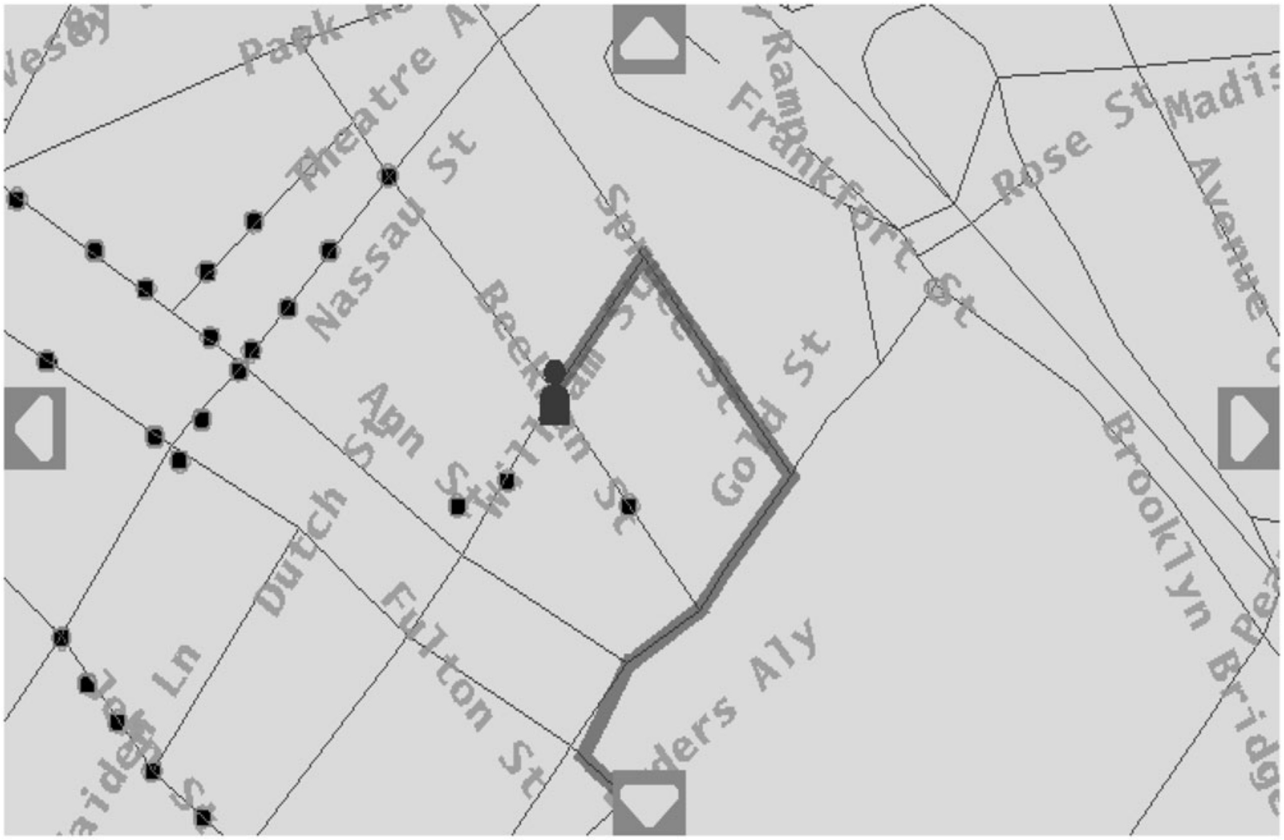
TERRESTRIAL REMOTE SENSING AND SURVEILLANCE

At the same time that the spatial resolution of satellite remote sensing systems is increasing, there is a parallel increase in the deployment of terrestrial sensing systems. For example, it is almost impossible to avoid the near-ubiquitous advertisements for miniature video cameras, seemingly intended for surreptitious spying. More overt uses are made of cameras to monitor the activities of workers in daycare centres and hospitals, as well as the more familiar bank and retail environments. Cameras in stores are increasingly being used not only to monitor customer behaviour to prevent theft but also to analyse consumers' decision-making and purchasing patterns (e.g., GMT Consulting 2000).

Terrestrial surveillance video systems are often rationalized for the sake of reducing terrorist and criminal threats. Britain is especially well covered, with at least 2.5 million surveillance cameras in place, which has led to one estimate that "the average Briton is now photographed by 300 separate cameras in a single day" (Rosen 2001, 41; also see Webster 2004). Cameras are not (yet) everywhere, but camera proliferation has been accepted by many urban residents as a fact of everyday life. Others, however, have developed a heightened sense of awareness and are resisting observation. The New York City Surveillance Camera Project, for example, sought citizen input to locate surveillance cameras in Manhattan that record public areas. These data are made available to the public by camera type (stationary or rotational) in map format at the project's Web site (NYC Surveillance n.d.), and the same data are also used by the Institute for Applied Autonomy (IAA) in a project called iSee (IAA n.d.), which allows users to define routes through Manhattan that avoid known camera locations. iSee requires the user to specify an origin and destination for the trip by clicking on a map. Software then computes a travel path that attempts to minimize observation at known camera sites (Figure 1). The way in which these conflicting goals (minimizing observation and distance) are traded off, however, is not revealed.

Video cameras are now widely deployed to control traffic signals, having replaced treadles and closed loop detectors in many urban areas. More controversially, cameras are increasingly used to detect and report traffic violations (notably speeding and failures to stop at red lights or to pay tolls). Red light camera services are often run by private companies under contract to local police departments. Grassroots efforts and private enterprise have already begun to map such cameras (as well as known speed traps) and are either making such information publicly available (Speed Trap Exchange n.d.) or using the information in products, such as Road Pilot (2005) or Origin blue i (n.d.), that alert drivers to oncoming cameras and traps using a combination of digital map databases and onboard global positioning system (GPS) technology.

Many surveillance cameras are stand-alone units. But networks are unifying image collection and analysis capabilities. Many people were surprised to see the sequence of images captured of Muhammad Atta and his accomplices during the day before, and morning of, the September 11 attacks on the World Trade Center in New York. Images from ATMs, gasoline purchases, and airport security were quickly assembled to retrace an activity path. If such images are linked to biometric and face recognition software, as was done at Super Bowl XXXI, then a space–time activity path can easily be assembled. Though the implications of this are chilling (see, e.g., Gray 2003), it is certain that enabling technology (software and hardware) will continue to improve. The number of cameras emplaced will continue to increase, since prices are dropping for cameras and their network connections, especially as the wireless communications infrastructure develops (e.g., WiMax). The final component is the inexorable development of software technology designed to scan oceans of images, classify them, and apply time and space stamps, thus supporting the construction of interpolated space–time trajectories of individuals (Hägerstrand 1970; Kwan 2004).



Source: http://www.appliedautonomy.com/isee/

Figure 1. Screen capture for a path of least observation by CCTV cameras in Manhattan. Camera locations are indicated by dark point symbols; the computed path is indicated by the thick dark-grey line. Source: The Institute for Applied Autonomy, http://www.appliedautonomy.com/isee.

Individual-Level Surveillance and GIS

Remote sensing is clearly not the only geospatial technology being used to collect and analyse individual-level information. In this section we describe important trends in the use, and possible misuse, of individual-level data routinely stored in rapidly proliferating administrative record systems and data warehouses. These information resources can be linked and processed with GIS software to uncover information that many consider private.

There is no doubt that enormous quantities of information are routinely collected about individuals during the course of most days in technologically advanced societies. Different people, of course, have their own proclivities with respect to surveillance. Someone who never uses the Internet, conducts transactions in cash, and avoids public places might have an almost invisible presence in databases contrasted with an urban credit-card glad-hander who leaves a distinct digital path much like an ant's pheromone trail (for a short commentary on "digitally dropping out," see Koerner 2002).

Despite the apparent profusion of information collection activity, most data are now fragmentary and proprietary; if linked and unified, however, they can reveal considerable detail about individual behaviour. Geography, it turns out, is an excellent medium to support such data conflation activities, since one particularly important way that databases are integrated is through the presence of common identifiers: addresses and other location identifiers are present in most administrative record systems, and they serve as a unifying glue. Moreover, with the advent of free on-line address-matching capabilities, one need not have access to GIS software; the barrier to entry has been removed. In the following two sections we consider two aspects of geocoded (address-matched) individual-level information. First, we examine the feasibility of transforming a dot map, one containing no personal identifiers, into a list of addresses that can be linked with other data sources to violate privacy assumptions. We then turn to a discussion of emerging

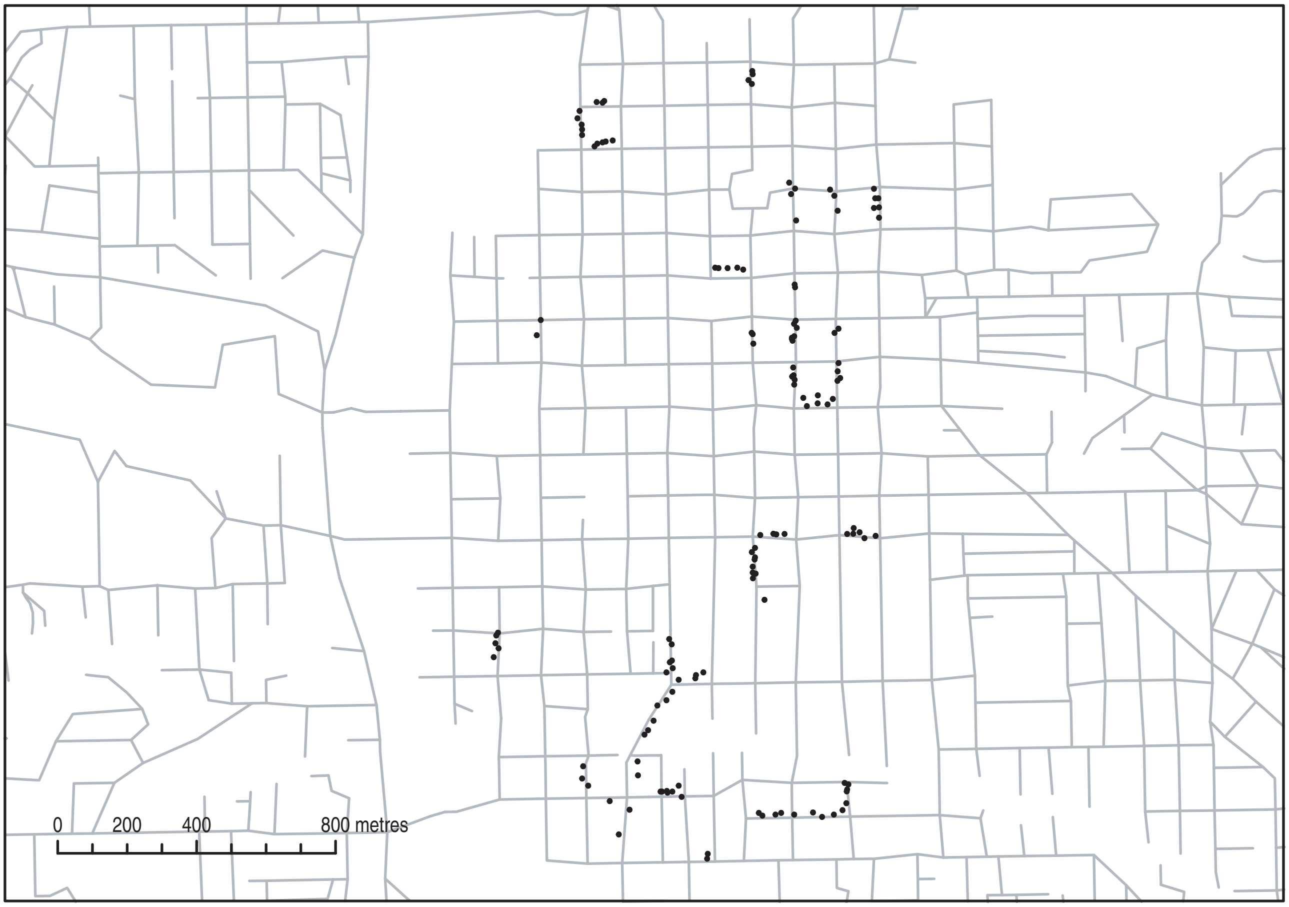


Figure 2. A dot map of addresses in Iowa City, IA, USA.

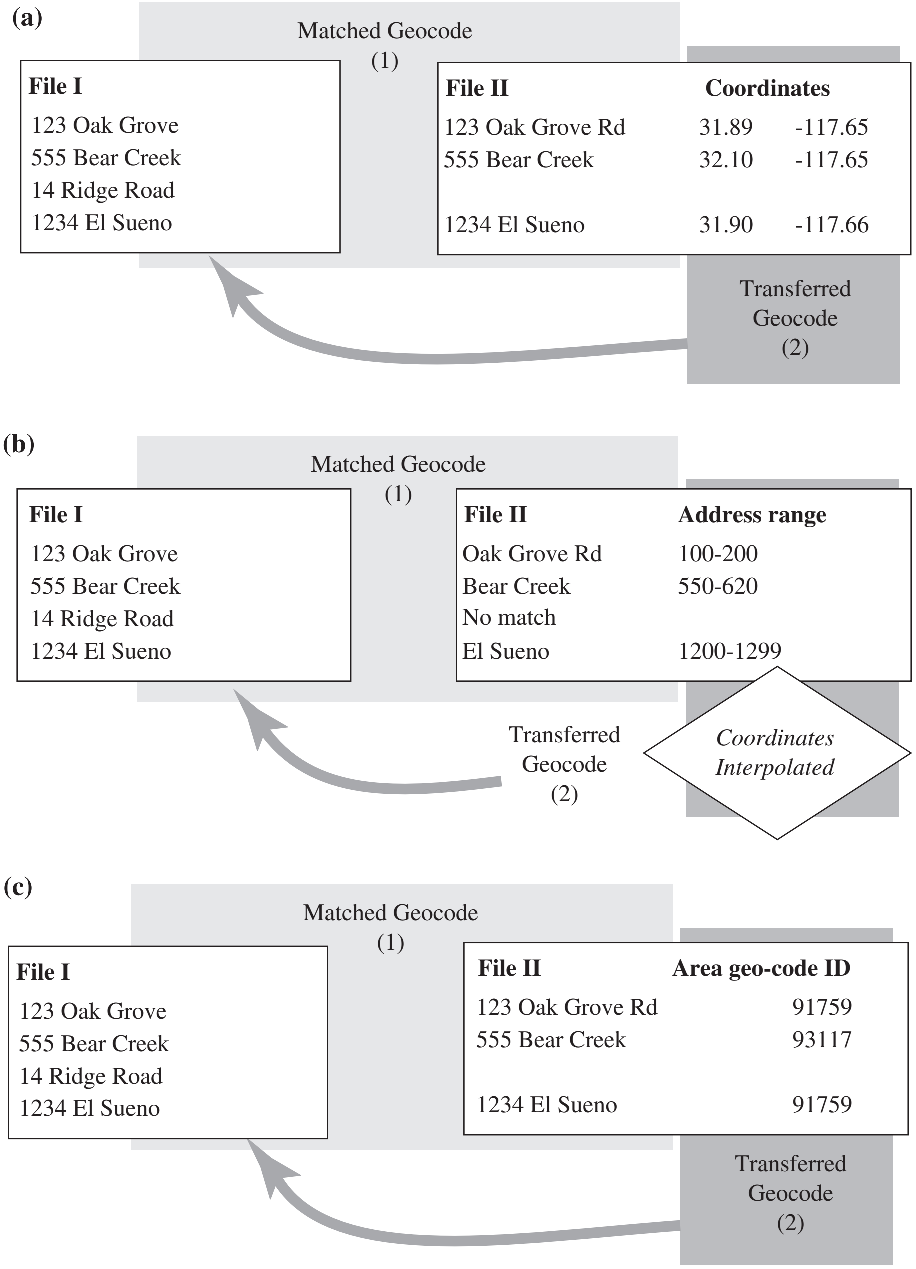
privacy aspects of a nascent quaternary sector of economic activity known as location-based services (LBS).

INVERTING ADDRESS–MATCHING TRANSFORMATIONS

When data are integrated from various sources, the increasingly pervasive nature of GIS software has led to the common practice of creating maps from the results. This is, in fact, a key driver of the adoption of geospatial technologies in many commercial enterprises. It is not widely known that such maps can be "hacked" to allow individual-level information to be recovered. In a typical dot map, the information depicted has been rendered anonymous to a certain extent (Figure 2). Though producing such maps required considerable effort in the past, they can now be made easily using inexpensive GIS software and public-sector street network databases, such as the TIGER files created to support US Census data collection activities (Broome and Meixler 1990; Marx 1990) or similar files available from GIS data vendors. Many Web sites now support such activities as well. For detailed examples of how such linkages from individual-level data to geography can be established and used in different contexts, see Chakraborty and Armstrong (2001) and Rushton, Armstrong, and Lolonis (1995).

As Figure 3 shows, several approaches can be used to attach a geographic identifier, such as a coordinate or areal unit identifier, to a specific address. Figure 3a shows the establishment of a match between an input file of addresses and another file that contains a specific coordinate pair for each of these addresses. Such files, while rare in the past, have become commonplace through the widespread use of digital tax parcel maps and GPS receivers. A more widely used form of address matching is shown in Figure 3b. In this case, coordinate values are interpolated based on address ranges associated with each street segment. Finally, Figure 3c shows the assignment of an areal geocode to an address. This procedure is typically applied when observations are aggregated to areal units, either to mask individual identities or to compute rates.

One commonly observed practice hinders the recovery of individual-level information from dot maps: using each symbol to represent multiple instances of a phenomenon (see Mackay 1949). When there is a one-to-one correspondence between symbol and subject, however, the dot map creation process can be inverted to recover



File I
123 Oak Grove
555 Bear Creek
14 Ridge Road
1234 El Sueno

File II	Coordinates	
123 Oak Grove Rd	31.89	-117.65
555 Bear Creek	32.10	-117.65
1234 El Sueno	31.90	-117.66

File I
123 Oak Grove
555 Bear Creek
14 Ridge Road
1234 El Sueno

File II	Address range
Oak Grove Rd	100-200
Bear Creek	550-620
No match	
El Sueno	1200-1299

File I
123 Oak Grove
555 Bear Creek
14 Ridge Road
1234 El Sueno

File II	Area geo-code ID
123 Oak Grove Rd	91759
555 Bear Creek	93117
1234 El Sueno	91759

Figure 3. Three general methods of geo-coding. The first method (a) transfers an exact coordinate for each address; there is a one-to-one correspondence between addresses and coordinates. The second method (b) estimates geographical coordinate values by interpolating along a street segment according to a proportion of the address range. If an address is, for example, halfway in the address range for a segment, the geographic location would be halfway between the coordinates of the end points of the segment. The third method (c) assigns an area geo-code, such as a census unit or political jurisdiction, to an address. This enables geo-coded information to be used with statistical information in ecological analyses.

individual-level addresses with relative ease. These recovered addresses can then be cross-referenced with other databases (e.g., city directories, telephone directories) to reveal further details about personal identities. This is particularly true when address-matching software is used to create the dot map. Such maps even have a commonly employed name when they are used to represent individual objects or events: pin maps. Each virtual pin placed on a map might represent the location, for example, of a specific instance of a crime or the home location of a person who has contracted some contagious disease.

Consider the dot map in Figure 2 again. It was produced by selecting 100 individuals from a telephone directory.

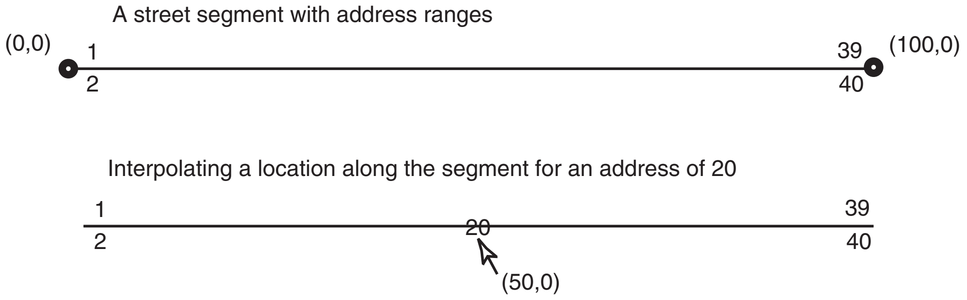

A street segment with address ranges
(0,0)
1
2
39
40
(100,0)
Interpolating a location along the segment for an address of 20
1
2
20
39
40
(50,0)

Figure 4. A more detailed example of interpolated address matching.

Their addresses were input into a database and then manipulated to produce a map using GIS software and a TIGER file. Despite problems that might be encountered during address matching (e.g., spelling errors and new residential development), with modern address-matching software it is often possible to match more than 90% of the addresses submitted for processing (see Rushton and others in press).

Uncertainty in recovering information from abstract dot symbols placed by address-matching software arises from four main interacting factors:

1. The process of creating a dot map often relies on interpolated locations. US TIGER files, for example, do not contain (*x*, *y*) coordinates for each residence. Instead they contain the coordinates of the end points (and some shape points) for each street segment, along with a range of addresses for each side. This information is then used to interpolate a coordinate for an address that is based on a proportion of the distance along the segment computed as a percentage of the address range. If, for example, the address range for a street segment begins at 2 and ends at 40, and if a candidate address were at 20, it would be placed approximately halfway along the street segment (see Figure 4). This approach ignores variations in lot sizes and other factors that cause irregularities in systematic address ranges.
2. The use of centreline files, such as TIGER, requires the displacement of symbols off the centre line to where they might be located in reality (Figure 5), though this information is not explicitly encoded in the file. Two parameters are normally used to perform this estimated displacement. The displacement (or offset) is usually a constant value (e.g., 10 m). This displacement can cause problems at the ends of street segments, so an additional parameter is used to move points inward toward the middle of the street segment. This parameter (a ‘‘squeeze’’ factor) is often set as a percentage (e.g., 5%). These two parameters are combined in an attempt to ensure that each dot is placed on the correct block (Figure 6).
3. The address ranges contained in the centreline files may be incorrect. In many places in the United States, TIGER files contain address ranges for each block face that are ‘‘hypothetical’’ in that they are round numbers (e.g., 100–198, 200–298) rather than the actual values present on the street segment. The use of these ranges does not cause problems if the goal of geocoding is solely to assign addresses to a particular block. However, if the goal is to allocate an address to its correct location along a block face, the use of hypothetical ranges increases the likelihood of large location errors, as shown in Figure 7. In that case a value of 39, which should be placed at one end of the street segment, is instead assigned a location nearer to the other end.
4. A final problem is a general one: map scale. If a dot map is produced using a small scale representation, the amount of area covered by a dot symbol will be quite large, and thus considerable errors in location determination can occur because each dot may literally ‘‘cover’’ multiple addresses. On the other hand, if the map is large scale, the dots will tend to be located much more precisely, if other factors are held constant. Consequently, a symbol will refer to a single address or, at least, to a very small number of them.

With the address-matched information represented as a dot map, we can then begin the process of inverse-address-matching. In some cases a map can simply be visually cross-referenced to on-line maps, such as those made publicly accessible for tax assessment in many municipalities. In other cases, a more involved procedure, using GIS software functions, may be required. In such cases, the process used to invert the address-matching transformation using a TIGER file, or a similar address-range-based file, can be specified as a sequence of steps:

1. The coordinate location of a dot is digitized, using the projection and origin of the source map.
2. Software then searches for the closest street segment (between street intersections) to those

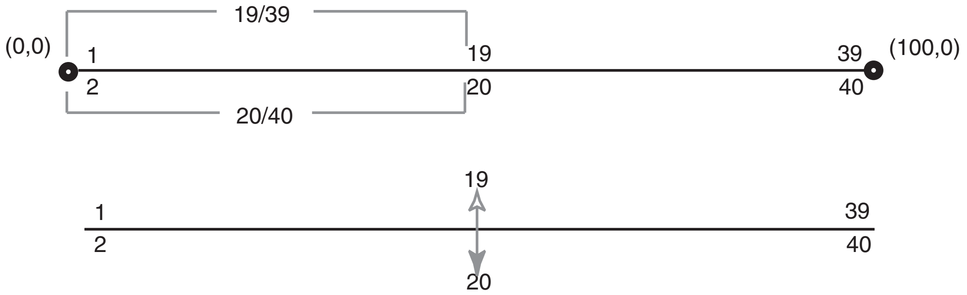


Figure 5. Problems can occur with addresses that are proportionately the same but on different sides of the street. The parity of the address is used to introduce an offset (e.g., 10 m) from the street centreline.

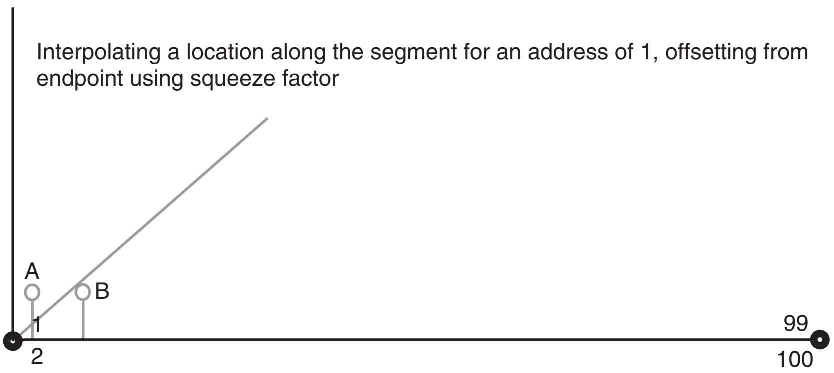

Interpolating a location along the segment for an address of 1, offsetting from endpoint using squeeze factor
A
B
1
2
99
100

Figure 6. The use of offset can introduce errors when addresses are located close to the end of a street segment; symbols may be displaced toward the centre of the segment using a percentage "squeeze" factor. The offset symbol (A) is closer to the (incorrect) vertical street than to the (correct) horizontal street. When the symbol is squeezed (B), it is moved away from the vertical street and is now closer to the (correct) horizontal street.

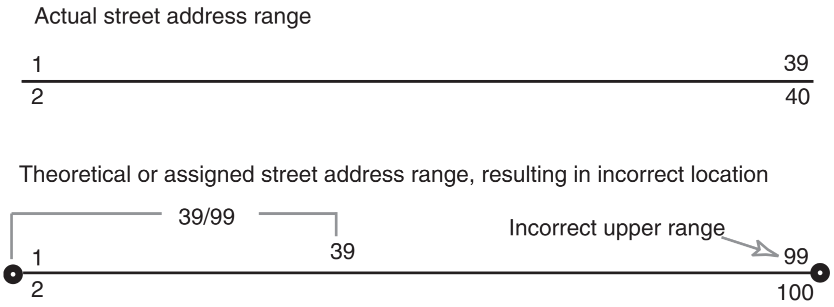

Actual street address range
1
2
39
40
Theoretical or assigned street address range, resulting in incorrect location
39/99
39
Incorrect upper range
1
2
99
100

Figure 7. In some cases "theoretical" address ranges are used, such as when addresses are given as multiples of 100 for each block. In reality, however, there may be a lack of agreement between such ranges and buildings. This can result in address-matching errors that shift the location of all symbols to the end of the street segment with the low value of the address range. In this figure, 39 is actually located at the end of the block (top), but it would be incorrectly assigned only approximately 40% of the way along the street segment (bottom) if a theoretical range were used.

coordinates and estimates the address as a proportion of addresses along the block face.

3. The address is then written to the screen or an output file, where it can be linked to other on-line data resources.

Largely as a result of the factors described above, however, uncertainty remains about whether the address obtained using this approach is the "correct" one. Nevertheless, it is clearly possible to perform this task. This fact has implications for the publication of maps containing data that can in some way be considered confidential or private. In such cases, masking techniques might be employed. One masking technique simply aggregates responses to areas, which induces a "needle in a haystack" problem. However, as described in the next section, if individual-level data must be mapped, a random displacement can be applied to each point to hinder accurate recovery of individual-level information (see Armstrong and others 1999; Kwan, Casas, and Schmitz 2004).

LOCATION-BASED SERVICES: A KILLER APP WITH AN APPETITE FOR PERSONAL INFORMATION

When cell phones came into widespread use in the late 1990s, an important problem developed. Cell phone users (in the United States) called 911 for emergency assistance; but these newly mobile individuals were no longer at a fixed location, and, in many cases, they were unable to describe their location accurately. As a result, emergency service providers were unable to render assistance. Because of the magnitude of this problem, the US Federal Communications Commission (FCC) has stipulated that activated cell phones must be locatable, either using triangulation of cell-phone packets based on signal strength (Hein and others 2001) or through the installation of GPS receivers. The FCC has recently taken an additional step, requiring that location information be provided for telephonic devices that use voice-over-Internet protocol (VoIP). Moreover, additional technology, such as assisted GPS (A-GPS; van Diggelen and Abraham 2001), is being developed to extend location determination capabilities to areas normally inaccessible to GPS signals, such as inside buildings and underground parking garages. These enhancements will soon make it possible for the location of a device to be monitored continuously at high levels of accuracy. This powerful ability, however, has begun to raise important public policy concerns about, and scientific inquiry into, individual privacy and surveillance (Applewhite 2002; Beresford and Stajano 2003; Myles, Friday, and Davies 2003). In this section we sketch out a general approach that would permit accurate E-911 service provision and provide context-sensitive information to those seeking LBS while simultaneously satisfying the conflicting objective of preserving location privacy.

Though inaccuracies occur for several reasons related to the satellite constellation, atmospheric distortion, and signal blockage, GPS receivers are able to calculate locations at high levels of accuracy under a broad range of conditions. To become useful to a LBS provider, however, a GPS-derived coordinate must be placed into a particular geographic context that is derived from the user's preferences as well as his or her site and situation. This can be accomplished, for example, by assigning a coordinate to its closest link on a street network or to a service area using a point-in-polygon function. Once a location has been established, a link to a contextual database is made and information is either served on request or pushed to the appliance. It is also at this "point" that information can be masked to preserve the location privacy of an individual using an LBS-enabled appliance. This mask would requires the consent of both a trusted location-based service provider and the user. E-911 service would remain unaffected, since the "raw" coordinate information would still be available for emergency services.

A mask, in this case, is a way to prevent accurate recovery of a coordinate location. The basic premise of the approach is that a location calculated for a LBS can be masked without substantially affecting the quality of the information provided to the user. As with inverse address-matching, such masks can be implemented using several methods, including aggregation and perturbation (Armstrong and others 1999). For a contextually adaptive mobile mask (CAMM), aggregation seems to hold promise, though a combination of aggregation and perturbation could be employed. The CAMM process would replace a coordinate location with an assigned one- or two-dimensional object. For example, a point location could first be assigned to a transportation link and then replaced with one or two topologically connected census block groups or tracts. The size of the area used could be a function of local population density (the context), time of day, location along a network (e.g., controlled-access highway), or other factors affecting location privacy.

The negative impact of masking is that the level of geographical specificity of services with respect to a current location is necessarily degraded. Thus, information about, say, locations of restaurants of a particular type within walking distance (established as a user-set parameter) may be inaccurate. But since users would have control over the level of masking invoked, they could adjust the mask to meet their goals and make trade-offs between the quality of service provided and their desire to maintain location privacy.

Concluding Discussion

The pace of technological change in advanced societies is increasing, and we are now truly on the cusp of living under the continuous gaze of government and business interests; digitally encoded information about many routine activities is being collected and used, with and without consent. Our goal has been to elucidate some of the increasingly significant impacts of geospatial technologies on what were once thought to be private day-to-day activities. Remote sensing technologies are increasing in resolution to permit the identification of everyday objects and individuals from space. Closer to home, effectively invisible technologies such as stealthy remotely piloted aircraft and closed-circuit television systems can now be used to conduct surveillance of individuals without their consent. Other geospatial operations can be applied to widely available digital maps to uncover the identities of the mapped and to monitor their proclivities.

As the capabilities of geospatial technologies are not generally known and understood by the public, many individuals will find it difficult to guard against unwanted intrusions into their personal lives. Many will remain permanently unaware of the surveillant power of geospatial technologies, while others will remain complacent about their use, perhaps until they are confronted with a personal fact gleaned about them from the bitstream. Individuals can try to opt out of the panoptic surveillance of geospatial technologies, but this will be difficult to accomplish. As was widely reported through a variety of news outlets in 1999, Scott McNealy, CEO of Sun Microsystems, responded to a question about on-line privacy in the following way: "You have zero privacy anyway. Get over it." It appears that we are headed to a similar place with respect to location privacy.

Acknowledgements

This publication was made possible, in part, through a Cooperative Agreement between the Centers for Disease Control and Prevention (CDC) and the Association of Schools of Public Health (ASPH), award number S-3111, "Prostate Cancer Geocoding: Assessing Fitness for Use." Additional support was provided by the National Science Foundation (SES-0345441 DMUU, "Statistical Disclosure Limitation for Geospatial Image Data").

Author Information

Marc Armstrong is a Professor in the Department of Geography and Graduate Program in Applied Mathematical and Computational Sciences at the University of Iowa, 316 Jessup Hall, The University of Iowa, Iowa City, IA 52242 USA. E-mail: marc-armstrong@uiowa.edu.

Amy Ruggles is a Senior Data Development Specialist at Rand McNally & Company, 8255 N. Central Park, Skokie, IL 60076 USA.

Note

1. For an idea of the extent of such use, enter into an Internet search engine the text string "IR marijuana cultivation."

References

Applewhite, A. 2002. "What Knows Where You Are?" *Pervasive Computing* (Oct.–Dec.): 4–8.

Armstrong, M.P. 2002. "Geographic Information Technologies and Their Potentially Erosive Effects on Personal Privacy." *Studies in the Social Sciences* 27/1: 19–28.

Armstrong, M.P., G. Rushton, and D.L. Zimmerman. 1999. "Geographically Masking Health Data to Preserve Confidentiality." *Statistics in Medicine* 18: 497–525.

Baker, J.C., K.M. O'Connell, and R.A. Williamson. 2001. *Commercial Observation Satellites: At the Leading Edge of Global Transparency.* Santa Monica, CA: RAND.

Bentham, J. 1843. *The Works of Jeremy Bentham, Published under the Superintendence of his Executor, John Bowring.* Edinburgh: W. Tait; London: Simpkin, Marshall.

Beresford, A.R., and F. Stajano. 2003. "Location Privacy in Pervasive Computing." *Pervasive Computing* (Jan.–Mar.): 46–55.

Broome, F.R., and D.B. Meixler. 1990. "The TIGER Data Base Structure." *Cartography and Geographic Information Systems* 17/1: 39–48.

Chakraborty, J., and M.P. Armstrong. 2001. "Assessing the Impact of Airborne Toxic Releases on Populations with Special Needs." *The Professional Geographer* 53: 119–131.

Curry, M.R. 1997. "The Digital Individual and the Private Realm." *Annals of the Association of American Geographers* 87: 681–699.

——. 1998. *Digital Places: Living with Geographic Information Technologies.* New York: Routledge.

Dash, S., R.F. Schwartz, and R.E. Knowlton. 1959. *The Eavesdroppers.* New Brunswick, NJ: Rutgers University Press.

Diffie, W., and S. Landau. 1998. Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge, MA: MIT Press.

Dobson, J. 1998. "Is GIS a Privacy Threat?" *GeoWorld* 11/7. Available at http://www.geoplace.com/gw/1998/0798/798onln.asp

——. 2000. "What Are the Ethical Limits of GIS?" *GeoWorld* 13/5. Available at http://www.geoplace.com/gw/2000/0500/0500g.asp

Dobson, J., and P. Fisher. 2003. "Geoslavery." *IEEE Technology and Society Magazine* (spring): 47–52.

Elden, S. 2003. "Plague, Panopticon, Police." *Surveillance and Society* 1: 240–53.

Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison.* Trans. A. Sheridan. New York: Pantheon.

GMT Consulting. 2000. "What Do You Really Know About Shoppers' In-Aisle Choices?" General Management Technologies: News and Ideas. Available at http://www.gmtconsulting.com/publications/ideas/consumer.htm

Goss, J. 1995. "We Know Who You Are and We Know Where You Live: The Instrumental Rationality of Geodemographic Systems." *Economic Geography* 71: 171–98.

Gray, M. 2003. "Urban Surveillance and Panopticism: Will We Recognize the Facial Recognition Society?" *Surveillance and Society* 1: 314–30.

Hägerstrand, T. 1970. "What About People in Regional Science?" *Papers of the Regional Science Association* 24: 7–21.

Hall, C.T. 1959. *The Silent Language.* Garden City, NJ: Doubleday.

——. 1966. *The Hidden Dimension.* Garden City, NJ: Doubleday.

Hein, G.W., B. Eissfeller, J.O. Winkel, and V. Oehler. 2001. "Determining Location Using Wireless Networks." *GPS World* 12/3: 26–37.

Holz, R.K. 1973. *The Surveillant Science: Remote Sensing of the Environment*. Boston: Houghton Mifflin.

Institute for Applied Autonomy. n.d. iSee. Available at http://www.appliedautonomy.com/

Jensen, J.R. 2004. *Introductory Digital Image Processing: A Remote Sensing Perspective*, 3rd ed. Upper Saddle River, NJ: Prentice Hall.

Koerner, B.I. 2002. "How to Disappear." *Wired* (July): 48.

Koskela, H. 2003. "'Cam-Era': The Contemporary Urban Panopticon." *Surveillance and Society* 1: 292–313.

Kwan, M.-P. 2004. "GIS Methods in Time-Geographic Research: Geocomputation and Geovisualization of Human Activity Patterns." *Geografiska Annaler B* 86: 205–18.

Kwan, M.-P., I. Casas, and B. Schmitz. 2004. "Protection of Geoprivacy and Accuracy of Spatial Information: How Effective Are Geographical Masks?" *Cartographica* 39/2:15–28.

Mackay, J.R. 1949. "Dotting the Map: An Analysis of Dot Size, Number and Visual Tone Density." *Surveying and Mapping* 9: 3–10.

Marx, R.W. 1990. "The TIGER System: Yesterday, Today and Tomorrow." *Cartography and Geographic Information Systems* 17/1: 89–97.

Monmonier, M. 2002. *Spying with Maps: Surveillance Technologies and the Future of Privacy.* Chicago: University of Chicago Press.

Myles, G., A. Friday, and N. Davies. 2003. "Preserving privacy in environments with location-based applications." *Pervasive Computing* (Jan.–Mar.): 56–64.

NYC Surveillance Camera Project. n.d. NYC Surveillance Camera Project homepage. Available at http://www.mediaeater.com/cameras/

Onsrud, H., J. Johnson, and X. Lopez. 1994. "Protecting Personal Privacy in Using Geographic Information Systems." *Photogrammetric Engineering and Remote Sensing* 60: 1083–95.

Origin blue i. n.d. "How Origin blue i Works." Available at http://www.originbluei.com/perform/howitworks.cfm

Road Pilot GPS. 2005. "Welcome to the Road Pilot GPS Website!" Available at http://www.roadpilot-gps.co.uk

Rosen, J. 2001. "A Watchful State." *New York Times Magazine* (7 Oct. 2001): 38–43, 85, 92–93.

Rushton, G., M.P. Armstrong, J. Gittler, B. Greene, M. West, and D. Zimmerman. In press. "Geocoding in Cancer Research: A Review." *American Journal of Preventive Medicine.*

Rushton, G., M.P. Armstrong, and P. Lolonis. 1995. "Small Area Student Projections Based on a Modifiable Spatial Filter." *Socio-Economic Planning Sciences* 29/3: 169–85.

Speed Trap Exchange. n.d. "Welcome to the Speed Trap Exchange." Available at http://www.speedtrap.org/

US Department of Commerce, National Oceanic and Atmospheric Administration. 2005. "Licensing of Commercial Remote Sensing Satellite Systems." Available at http://www.licensing.noaa.gov/faq.htm

van Diggelen, F., and C. Abraham. 2001. "Indoor GPS: The No-Chip Challenge." *GPS World* 12/9: 50–58.

Waters, N. 2000. "GIS and the Bitter Fruit: Privacy Issues in the Age of the Internet." *GeoWorld* (May). Available at http://www.geoplace.com/gw/2000/0500/0500edg.asp

Webster, W.R. 2004. "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK." *Surveillance and Society* 2: 230–50.

Wood, D. 2003. "Editorial: Foucault and Panopticism Revisited." *Surveillance and Society* 1: 234–39.

cartographica

the international journal for geographic information and geovisualization