GIS Technology: new threat to privacy, new promises for citizen empowerment. *

Pedro Ferraz de Abreu

Massachusetts Institute of Technology
Department of Urban Studies and Planning

pfa@mit.edu

Abstract

When Geographic Information Systems (GIS) emerged, some authors have argued that the privacy issues raised by the advent of the GIS technologies are essentially the same as those raised by electronic databases of personal information. This perception is not hard to understand, considering that most of the issues raised by the advent of electronic databases are still currently challenging us, and have yet to find an adequate response within a legal and institutional framework inherited from an Era when paper based records and transactions were the (only) norm. In my view, these authors fail to realize that the extended capability of the GIS raises some new issues, and brings others to a new depth. What privacy issues are specific to GIS ? Can GIS endanger or instead help to protect and enhance privacy rights? How? The concept of privacy rights is cultural dependent, and it is reflected in the differences in legislation from country to country. What are the main trends? How does it affect the impact of GIS in privacy?

The context

Even authors, like Bishop Dansby, that admit a difference, still minimize the special role that GIS may play in issues like privacy and others: "*it is more appropriate to address all information technologies together, since GIS is only a subset of information that can impact privacy*" [Dansby 91]. Since any GIS

* Submitted in 1996. First presented at GE, MIT-DUSP, 1993

contains one form or another of an electronic database, it is only natural that they share privacy problematic; but, In my view, these authors[1] fail to realize that the extended capability of the GIS raises some new issues, and brings others to a new depth.

It is important to begin by clarifying what do we call a GIS, and what do we understand as a privacy problem. The hidden assumption that we are all talking about the same thing, or that the differences between definitions are irrelevant to the point in question, is probably one of the reasons of existence of these contraditory views.

1. The definition of a GIS; **2**. The concept of privacy; **3**. Tradeoffs privacy vs. free/easy access to electronic data; **4**. Tradeoffs privacy vs. free/easy access to GIS-based data; **5**. Cultural differences towards privacy.

1. The definition of a GIS .

Dana Tomlin [Tomlin 90] views GIS as a facility for preparing, presenting, and interpreting facts that pertain to the surface of the earth. Beng Chin Ooi [Ooi 90] defines GIS as database systems that allow the manipulation, storage, retrieval, and analysis of geographic data and the display of data in the form of maps. For Lyna Wiggins and Steven French [Wiggins, French 91], GIS combines the database management system's power to store, retrieve and analyze information with the ability to produce and manipulate the graphic elements of a map.

Laserna, Landis and others [Laserna, Landis 89] have identified five basic analytical functions that should be supported by a GIS package: forward data query, backward data query, polygon overlay, point-in-polygon overlay, and

[1] This article relies on extensive citations of many key authors, specially in domains like legal frameworks. Despite my critical views on some of these articles, they must be credited as an important contribute to this paper, besides the standard acknowledgment in the references section.

buffering. On the other hand, Les Worral [Worral 91] complains that currently GIS only provide some geometric tools for spatial analysis, compared to its full potential.

For all the different focus, these and other authors agree on the following: 1) GIS have some form of DBMS (database management system) built-in; 2) GIS handle cartographic data; 3) GIS have the capability to link spatial with aspatial data; 4) GIS have capability beyond DBMS to analyse spatial data and spatial relationships.

It is this extra capability of GIS to answer from the basic questions "Where is...", "What is at" [Dueker 88] to more sophisticated series of spatial manipulations that generate new information [Cowen 87], that is at the source of the new privacy issues raised by GIS. The most important of these is the new capability of GIS to provide information on the physical location of objects and individuals, and cross-reference / match (by means of this now known location), with a wealth of other information previously associated only with the location (or neighborhood), and not with the individual or object, where before (without GIS) this localization and cross-georeferencing was either impossible or too cumbersome or expensive to be practiced. This undoubtly has created a new perceived threat of invasion of privacy by computers.

It may be argued that one could obtain similar results through good use of DBMS data manipulation languages. On one hand, linking tabular data to cartographic data, or even to images (like remote sensing grid data in the case of raster GIS), is no trivial task and demands special handling of the storage, retrieval and manipulation. On the other hand, extending DBMS with routines in order to handle typical GIS queries, like the classes of queries suggested by Burrough [Burrough 86], "where is A in relation to place B?", "what objects are next to objects having certain combinations of attributes?", "what is the result

of intersecting different layers of polygons representing different attributes?", etc., is in fact one form of producing GIS software. In other words, if we try to extend more and more some DBMS software to handle what a GIS handles, in the end we have a GIS software, not anymore a plain DBMS. This is for example the approach taken by those who work on special extensions of structured query languages (SQL) to handle spatial relationships (e.g. adjacency), like GeoQL [Sacks-Davis 87].

There is no doubt in the minds of many authors that "*GIS is different from conventional DBMS in many ways*" which imply special programming [Ooi 90] [Davis, Palat 85]: the data types consist of complex objects, like lines and regions; spatial orderings of spatial objects are harder to define; the entities relationship (representation with Chen's entity-relationship model) is more complex in the sense that it must be computed or inferred. The differences are so extensive that in fact many GIS came to exist not as extensions of DBMS, but as extensions of image-processing programs, better prepared to handle raster transformations, or CAD/CAM, an easier transition regarding vectorial representation of topologies.

D.J. Cowen best sumarizes these arguments, when he writes that "*a true GIS can be distinguished from other systems through its capacity to conduct spatial searches and overlays that actually generate new information*" [Cowen 87]. But this is not all. GIS have also the ability of visualizing spatial data [Marble 87], particularly maps.

Visualization is important, because our eyes (the only "peripherical" sensor organ that is actually part of the brain) enable our brain to perform spatial analysis on its own with image-based data representation formats [Fischler 87]; a much harder or even impossible task with other data representations, for instance tabular files. By facilitating map transformations, GIS multiplies

the power of a map representation by several orders of magnitude. As H. Archer said, "once the map is in the computer, you can do an awful lot more than just plot it out again" [Archer 88].

2. The concept of privacy.

In the USA, the constitutional right to privacy is, as Justice Brandeis once said, *"the right to be left alone - the most comprehensive of rights and the right most valued by civilized men"*. However, the right to privacy is not explicitly granted by the US Constitution, and it is the interpretation of the Supreme Court that has granted this right based sometimes on the First Amendment or the Fifht Amendment (sometimes the Fourteen), but usually rooted in the Fourth Amendment of *"protection of persons, places, papers, and effects against unreasonable searches and seizures".*

So far, this seems to be relatively independent of technological issues. But in 1967, the US Supreme Court (*apropos* ruling a warrentless wiretapping as unconstitutional, Katz versus United States) while holding that the Fourth Amendment protects people, not places, set forth a standard for determining constitutionally protected *"zones of privacy"* [Berman 89]: whether the expectation of privacy in the area to be searched outweights the government's interest in searching that area. As several scholars pointed out [Marx 86, 90], [Berman 89], the problem with the *Katz* formulation is that its related standard - a "reasonable expectation of privacy" - creates a technologically dependent standard of privacy. Berman points that the Court in later cases "*often determined that an individual's privacy had not been violated by certain intrusions because society's 'expectation of privacy' had been persistently lowered by the circunstances of modern existence*" [Berman 89].

It follows that technological advances in gathering and processing

information, as an obvious "circunstance of modern existence", have in fact the consequence of lowering the court's standard of "reasonable expectation of privacy", as indeed it happened.

Because GIS extended the already impressive capabilities of electronic databases, the erosion of court protection over individual privacy rights goes several steps further. Under this standard, there is the risk that individuals fighting data processing initiatives that will potentially identify their address and relate it with potentially sensitive private information -- such as a economic profile (e.g. wealthy), a demographic profile (e.g. senior citizen, retired), a gender profile (e.g. female), a seazonal profile (e.g. months of less consuption of utilities, reflecting period of absentia), etc. -- may not object anymore on the grounds of invasion of privacy, since the recent proliferation of GIS tools and geographic data in private and public hands cannot give them anymore a "reasonable expectation of privacy".

Finally, this court privacy standard is further downgraded because GIS technologies brought with them the proliferation of new data. Not only old data becomes a new threat to privacy (because of the new ease to link several pieces of it, pieces that by themselves were harmless), but also new types of data are now colected, particularly geographic related data, because GIS provides a new convenient and (relatively) inexpensive tool to make good use of it. Furthermore, the role of GIS in coordinating and integrating existing data bases is increasing dramatically [Challender, North 91]; by providing a more powerful and efficient front-end to huge corporate databases, GIS is acting as an acelerator of the integration and cross-referencing of a variety of data sources.

3. Tradeoffs privacy vs. free/easy access to electronic data.

Despite these real threats to privacy, it would be a mistake to adopt a plain reactionary view and a strategy of systematic censorship, control and limitation on data gathering and processing. On one hand, it would be hard (and expensive) to achieve and enforce such strategy, and on the other hand it would banish many useful applications of the new technologies. As it often happens, the technology not only raises problems, it also brings the means to tackle them successfully. In this case, a clever use of the potential of information technologies and easy access to electronic data can act as an instrument of citizen control (or accountability checking) over government and corporation activities, verify the content of the information circulating that might affect individual lifes, thus directly or indirectly strengthening privacy.

US Federal law reflect this effort to balance the concern for privacy (Privacy Protection Act) with the need to allow public access to information (Freedom of Information Act). Because of several loopholes and gaps in this legislation (the federal act refers primary to actions at federal level and tends to exclude state, local, and private sector activities), several states introduced legislation of their own, tilting the balance towards one end or the other.

In Delaware, for instance, the law explicitly states that "*it is vital in a democratic society that public business be performed in an open and public manner so that our citizens shall have the opportunity to observe the performance of public officials and to monitor the decisions that are made by such officials in formulating and executing public policy, and further, it is vital that citizens have easy access to public records in order that the society remain free and democratic. Towards these ends, and to further the accountability of government to the citizens of this state, this chapter is adopted and shall be construed*" [Delaware Code Annotated Title 29 & 10001]. Several authors [Dangermond 88] [Marx 90] defend the importance of public access to electronic data to hunt a wide variety of illegalities, threats, hazards, patterns

of environment decay, inconsistencies of government, etc.

So the tradeoff here is between limiting and controling general access to information to protect privacy, and allowing the very same access, to further the cause of democratic accountability.

Another example of tradeoff is the compilation of databases of mailing lists by commercial entities, from data gathered through credit card buys, etc., and then sold in the market to anyone interested. On one hand, it allows citizens the convenience of mail shopping, and to obtain special dedicated services and information, making possible and efficient a market responding to variety and specific wishes (tailored market), as opposed to the times of mass production of T models. But on the other hand it also generates indiscriminated pressure to consume (e.g. targeting children), piles of unwanted junk mail, and the nuisance and sheer harassment of telemarketing, particularly by automated recordings run by computer programs. A real life example: during my Ph.D. General Examination, I was twice interrupted by the telephone ring, only to hear a recording asking me marketing questions. I can tell by direct experience how disruptive and annoying it is to be the target of this practice. According to Gary Marx [Marx 90], the latest tendency is to interpret the law as only obligating the data collector entity to inform the citizen if information like their address and telephone are going to be used for any purpose different of what is expressed.

Another example of tradeoff is the increasing centralization and generalization of use of individual identifiers, such as the social security number (SSN). The problem of a unique, universal, identifier was raised to new heights with the advent of DBMS technology, because it allowed quick inexpensive computer matching of multiple files indexed by such unique identifier. In several countries the legislative bodies passed laws explicitly

banning a universal identifier, on the grounds of endangering citizen privacy and facilitating all sorts of abuse. In the USA, by law, the only agencies that can demand a SSN are the social Security Administration, the IRS, employers, banks and the military. Other agencies such as credit bureaus, insurance companies, police departments and hospitals have no legal authority to request it. However, the practice of asking for the SSN is widespread, and many people do not realize the implications of satisfying the request.

The advantages of a unique identifier are obvious, in terms of the added value for many pieces of information by virtue of the new cross-reference capability. One example is the use by IRS to detect tax fraud, which is in principle an activity of great interest for the whole society, and for low-income citizens in particular. But in general this is a one-sided advantage, since governments and corporations are more likely to profit from it than private citizens, and frequent cases of police abuse raise the specter of the Orwelian "big brother" society. Also organized crime finds such low-integrity schemes as a social security number a "*positive boon in its aims to legitimize false identities*" [Clarke 91].

The press is full of examples of citizens that were harassed by the IRS or their bosses by virtue of fraudulent use of their SSN by someone else. Some authors attribute the increasing abuse of SSN to two main factors: undocumented immigrants, and the business world's increasing use of the SSN as a universal ID [Berman 89] [Clarke 91].

In general, the Privacy Act limits the use of the SSN for identification purposes but now courts are tilting towards other end, after enacting the Tax Reform Act and the Income Eligibility Verification System, with explicit recourse to computer matching through the use of SSN. It is interesting that the "tilting" was so notorious, that it was later felt the need to introduce an

amendment to the Privacy Act, The Computer Matching and Privacy Protection Act (1988), in order to balance the evident consequences of the new computer technology.

Yet another interesting tradeoff regards the collection of credit information by private business, that is then sold to other business and institutions, with far reaching consequences for the individuals listed.

On one hand, it may be argued that credit information is crucial in a market economy, and therefore contributing for the good health of the economy. But on the other hand, the advantages for individual citizens are minimal compared to the advantages for business, and the risks and consequences of mistakes are in general far more devastating for individuals than for business.

To make things worse, the proliferation of these credit bureaus makes harder for citizens to check the contents of credit reports, and puts the burden (and respective transaction costs) unfairly on individuals. Gary Marx refers that as if it was not bad enough to take an individual's personal information (e.g. data on credit, employment, consumption, life style, age, marital status, address, telephone and social security number) without permission and sell it, several credit bureaus actually make money selling back to the individuals a copy of their own record. "*It's even worse, though, when this is done with legal immunity for the seller for any invasion of privacy, defamation of character or negligence the subject may suffer on account of a false credit report. Then to turn around and charge the subject a fee to see what is that the company is telling others is truly outrageous*" [Marx 89].

In 1970, the US Congress passed the Fair Credit Reporting Act, and later (1978) the Right to Financial Privacy Act. The act requires the agencies to allow consumers to review their own records and correct inaccurate information,

and prohibits credit bureaus to disclose records to anyone other than "authorized customers" [Berman 89].

In general, the law tries to achieve some balance between the right to access information, business and state interests, and privacy concerns. But the overall pattern is that the burden of protecting privacy is left to the initiative (and imagination) of the citizens. Also, although many of these laws explicitly recognize their applicability to computerized information, most were enacted prior to the recent revolution in information technologies and the new ability to manipulate information.

Following the above considerations regarding the mentioned tradeoffs, I would say that the law is more protective towards privacy (in descending order) on credit reporting, privacy protection on free access to information, mailing lists, and unique identifier.

The more burdensome (in terms of real enforcement) are, again in descending order, privacy protection on free access to information, credit reporting, unique identifier, and mailing lists. The reason why I consider the unique identifier tradeoff as the less protected, is because it is the issue more easily dependent from Federal policy and actions (in this case with a strong contradictory interest, tax control), since by its own nature it depends on the degree of centralization intended by a central power, with the means and resources to do it. Credit reporting is fairly well protected by law, in terms of providing the most clear framework (with less contradictions), but poorly enforced.

4. Tradeoffs privacy vs. free/easy access to GIS-based data.

Practically all the above tradeoffs apply to GIS based data, but in some

cases with a new twist.

For instance, regarding the Privacy Act and free access of information, the power of GIS to handle geographic data raises a new dimension of concern. During the multiple debates around this act and amendments, representative Frank Horton of NY refers explicitly to this concern: "*one of the most practical of our present safeguards of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard*" (US Congress, 1966). The plan of a central data bank was then abandoned; but nowadays, with GIS technologies spreading fast, there is no need anymore for a "central data bank" to achieve the retrieval of these pieces "scattered across the geography", neither to link geography to pieces of information. Consequently, neither is the simple refusal of a central data bank enough protection regarding privacy.

In question is again the particular ability of GIS to locate physically individuals and objects, from apparently harmless information. For instance, S. Aronoff thinks that the ability to produce a comparative map of the reproduction of dogs in a certain area (with the apparently harmless objective of finding which neighborhoods have higher rates of incidents of dog bites) can contribute to lower real estate value, damage the image of these neighborhoods and indirectly the image of the real estate owners [Aronoff 89]. The same author also refers to the ability to visualize small areas with higher concentrations of young single females as a potential nuisance.

Naturally, the tradeoff is with the positive applications enabled by GIS: Valerie Aillaud cites the case of spatial queries leading to the determination of the areas with high percentage of apartment buildings built before 1948 in France (predicting the presence of lead), from geo-referencing different census

files and tax information [Aillaud 92]. Dangermond refers to a citizen group in the city of Los Angeles that sued the city for having its general plan inconsistent with the legal zoning maps. This was discovered by overlaying land use zoning maps on top of the general plan and finding parcels which were zoned residential, but which had plans for being commercial [Dangermond 88].

Conversely, GIS technology also facilitate new solutions for these contradictory interests, by the ease of aggregation operations, that allow for legal measures establishing levels of aggregation open to public access, diminishing consequently the threat of individual localization.

Another example of a different twist to an "old" issue, is the mailing lists' tradeoff: the added ability of linking address information to geographic coordinates and then proceed to other spatial analysis of the data available, increases several times the chances of becoming a special target of special interests or sellers, in this case door to door marketing efforts in certain areas, besides telemarketing. Gary Marx acknowledges this effect: "*Mass marketing is inefficient and economic viability requires the pinpoint or 'segmented' marketing that computer analysis now makes possible by using 'point of sale' information*" [Marx 90].

Again the issue is that geographic-based matching is much more efficient than cross-referencing flat files indexed by address, an address which rarely is found in any compatible format. With the advent of GIS, public files dedicated to this geo-referencing (from address to geographic coordinates and vice-versa) are being produced and updated, like the TIGER files covering all USA, and standardization of address representation is gaining ground.

Other facets of these tradeoffs enhanced by GIS are the matching of records on applications to new jobs, front-end audits , school records, etc. , with

respective legislation (such as the Family Educational Rights and Privacy Act), trying to balance the right to know with the right of privacy [Clarke 91].

Finally, it is interesting to refer to a future development that is very likely to reformulate a tradeoff so far not directly related to GIS: the caller-ID technology.

Currently, in areas where it is offered, caller-ID can reveal the caller's phone number without his/her knowledge or consent. In some states, the phone companies must offer the ability to individual subscribers to block this information in all or some of their calls - for a price. In some cases, like Boston, the phone companies just gave-up in all of offering the service, when faced with such demands (they are now implementing it, but only after failing the lobbying efforts, causing a delay of several years). In others, they are actively leading away subscribers to block information to all calls by default, on the grounds that it may undercut the ability of emergency services to locate them in time to save life or property (Again, I had direct experience of this practice). This half-truth is obviously motivated by the fear of mass blocking neutralizing effectively any appeal to subscribe to this service.

The caller-ID has some evident advantages, even in terms of privacy - for instance, in deterring harassment calls. On the other hand, it undermines an instrument of communication in many cases where anonymity is not only reasonable but desirable [Marx 90]; and again multiplies by several orders of magnitude the nuisances of telemarketing. But this is only an emerging technology. There is already some reverse directories being offered by a fee that allow to obtain directly a name and address from the telephone number captured by the caller-ID. In my opinion, it will be just a matter of time before the proliferation of GIS software dedicated to further use this information in order to produce geographic matching with other files, presumably in real-

time. Undoubtedly, the damage to privacy will be even deeper.

Following the above considerations regarding the mentioned tradeoffs, I would say that when considering the use of GIS, the need of more privacy protection is (in descending order) on privacy protection on free access to information, mailing lists, credit reporting, and unique identifier. The more burdensome (in terms of real enforcement) are, again in descending order, privacy protection on free access to information, credit reporting, unique identifier, and mailing lists.

Note that in my view, the protection against a unique identifier is of less and less relevance, given the multiple abilities (enhanced by GIS) of cross-referencing and identifying individuals and objects. In this regard, what gains importance is not so much the control of the information open to public access (harder and harder to enforce), but the real ability of citizens to check all the information about them (and correct, or request to eliminate) easily and without cost. The ranking also reflects my view that regulating mailing lists becomes a more serious problem with GIS then with plain DBMS. As for the level of costs and difficulties to enforce, my view is that they will change, but it is not a clear case if the changes will affect my previous ranking for non-GIS settings.

5. Cultural differences towards privacy.

The situations and attitudes in many countries are very different from the USA case. Unlike in the US, where most protections are relative to how data is treated once they are collected [Marx 90], many European countries attempt to regulate data collection and use. The overall contrast can be expressed (even at the risk of oversimplification) the following way: in the US, data collectors are given more or less free hand in gathering information ("do first

and ask later"), and then each time problems arise (or citizens are successful in raising political attention), the state (federal or local) will introduce some regulation. In most Europe, political tradition and ideology induces the state to formulate a web of regulations forcing data collectors to "ask first and do later", and then, when a problem arises (with evolving technologies, for instance), local institutions and business press for regulation reform (or de-regulation).

This different tradition reflects also upon the strategies and approaches to handle tradeoffs of privacy vs. right to access information. In USA, the tradition is clearly one of relying more on market forces to find the right balance - and it is up to citizens to mobilize and try to counteract the dominant tendencies, if they are displeased by them.

After all, given the free market, one can buy technologies to prevent privacy invasion; personal information becomes just a commodity, to be sold like any other [Marx 90].

However, this strategy became more complex with the gradual transformation of the economy into an information economy, and the increasing economic value of public and private information. On one hand, the Free Information Act mandates public services to produce and maintain information, which is an increasingly costly operation, and then give it for free or only a nominal fee. On the other hand, some of this information is so valuable that private business can now reap huge profits just by repackaging the very same information obtained through this right, and resell it (some times back to public agencies!), even with little added value. Roitman comments on how the law (except in rare cases) fails to recognize the commercial value associated with computerized data bases and sophisticated information systems [Roitman 88].

The result is a mix of copyrights mess (further complicated by the need to separate software and hardware media from the actual "content" of information), with the pervasive questioning of old untouchable assumptions like the sovereign immunity.

The doctrine of sovereign immunity is an ancient one dating to the earliest days of the British monarchy. Sovereign immunity meant that the king as the embodiment of the state, could do no wrong, and could not be held accountable for his actions either good or bad. In current USA, it came to mean that the state could not be sued without its consent. Local governments can be sued without consent, but liability is restricted.

The problem arises when the public sector tries to introduce the most common-sense solution: to update charged fees for information, in order to reflect not only media costs but also capital investments and maintenance costs. Puissegur, among others, asks whether or not charging for public information will eradicate the government's defense of sovereign immunity for liability for errors it commits which harm a citizen [Puissegur 88].

European countries have their own headaches with the new emerging technologies. Taking the example of France, the strategy being followed involves the creation of special state organisms and special detailed regulations. The CNIL (Commission Nationale de l'Informatique et des Libertes), a super-committee within the Justice Ministry, supposedly independent but with members designated from the Parliament and other state organisms, is a mix of a supreme court specialized in information and privacy, and an executive body with vast powers regarding the authorization or destruction of information systems [Delahaye 87]. So far, its existence, composition and powers are generally accepted by the public.

As for regulatory strategy, it is directed towards avoiding the constitution of files identifying individuals and their address ("informations nominatives"), or the characterization of populations at fine levels of disaggregation, unless by the respective state organisms relevant to the information, and only used for its specific purpose. It has an impressive level of detail. For instance, the cross-reference of more than 4 variables is explicitly forbidden; if one of the variables cross-referenced has more than 10 modalities, the system cannot cross-reference more than 3 variables, etc., etc. [Aillaud 92].

Naturally, problems arise from this rigid framework. Recently, local governments (which in France have a certain autonomy in terms of local taxation and revenue), asked the CNIL authorization to adopt GIS software that would help them increase local tax revenues, both by fraud detection and better property evaluation. Because it involved cross-referencing several distinct files "property" of different national ministries, and because it involved spatial analysis at a disagreggated level allowing the identification of individuals and objects, the CNIL refused. Instead, it proposed a modified system allowing a similar analysis but at a much more aggregated level - totally useless for the local governments. Consequently, a fierce debate is in course, regarding local vs. national prerogatives, autonomous use of GIS software, etc.

It is an interesting contrast to observe that the debate in the US over a similar issue - use of GIS for local taxation purposes - is conducted over a totally different ground. For instance, Earl Raymond's article "Old Tax Maps: Are they Suitable for GIS?" [Raymond 90], reflects the dominant concerns of accuracy and detail of information.

The question is not whether using GIS to cross-reference tax related information will harm privacy, and how to get permission (!) to do it, but

whether the old maps are good enough for GIS, and whether more and better information can be obtained by the use of other modern technologies, like satellite-based Global Positioning Systems. If and when privacy is damaged by this dynamic, well, it will be up to the good old citizens of New England to first realize that damage was done, second to think of how to counteract, and third to engage in a campaign towards that end.

The new technologies pose therefore another challenge, and offer another promise: a tradeoff between one and the other extreme strategies.

References

[Aillaud 92] "La protection des donne'es personelles dans les SIG mis en oeuvre par les collectivites locales," Valerie Aillaud, Memoire de DESS, Institut francais d'Urbanisme, Universite de Paris 8. 1992.

[Archer 88] "Providing and Selling Access to AM/FM Data," Hugh Archer. URISA' 88, vol. IV pag. 348-357 . 1988.

[Aronoff 89] "GIS: A management perspective," S. Aronoff, WLD Publications, Ottawa, Canada. 1989.

[Berman 89] "A Federal Right of Information Privacy: The Need for Reform," Jerry Berman, Janlori Goldman. Benton Foundation, Project on Communications & Information Policy Options. 1989.

[Clarke 91] "Information Technology and Dataveillance," Roger Clarke in Computerization and Controversy: Value conflicts and Social Choices, Academic Press, San Diego, 1991.

[Cowen 87] "GIS vs. CADD vs. DBMS: What are the differences?," D.J. Cowen. Proceedings of GIS/LIS'87 Conferences, sponsored by ASPRS/ACSM, URISA, and AAG, pp46-56. S. Francisco, 1987.

[Dangermond 88] "Who is designing geographic information systems for the public?", Jack Dangermond, Environmental Systems Research Institute. URISA, vol III, pag 37, 1988.

[Dansby 91] "Informational Privacy and GIS," H. Bishop Dansby. American Cadastre, Inc. URISA, vol IV. pag 18-28, 1991.

[Davis, Palat 85] "Data Base management for geo-data. Tech. Rep 85-17, Univ. of Alberta, Edmonton, Canada. 1985.

[Delahaye 87] "Informatique et Liberte," H. Delahaye, F. Paoletti, La Decouverte, Paris. 1987.

[Fischler 87] "Intelligence: The Eye, The Brain, and The Computer," Martin Fischler, Oscar Firschein. Addison-Wesley, 1987.

[Haskins 91] "Empowering local land use planning officials through use of land information system technology," Brenda R. Haskins , Lucy A. Buchan, Peter G. Thum , Stephen J. Ventura. URISA 1991.

[Laserna, Landis 89] "Desktop Mapping for Planning and Strategic Decision Making," Roberto Laserna, John Landis, and Strategic Mapping, Inc. S.Jose California. Strategic Mapping, Inc. 1989.

[Marble 87] "The Computer and Cartography," D.F. Marble. The American Cartographer, 14, pag. 101-103. 1987.

[Marx 86] "The iron fist and the velvet glove: totalitarian potentials within democratic structures", Gary T. Marx, MIT, in "The social fabric: Dimensions and issues", edited by James Short, 1986.

[Marx 89] "For sale: Personal information about you.", Gary T. Marx, MIT. The Washington Post, December 11, 1989.

[Marx 90] "Privacy and Technology", Gary T. Marx, MIT. The World & I - Currents in modern thought - privacy, 1990.

[Ooi 90] "Efficient Query Processing in Geographic Information Systems,"

Beng Chin Ooi. Springer-Verlag. 1990.

[Puissegur 88] "Does charging for public information eradicate the defense of sovereign immunity," Alma Puissegur. URISA, vol IV, pag. 358, 1988.

[Raymond 90] "Old Tax Maps: Are they Suitable for GIS?," Earl Raymond. Remote Sensing and Database Development News, winter 1990.

[Roitman 88] "Public records laws: a proposed model for changes," Howard Roitmen. URISA vol IV, pag. 338, 1988.

[Sacks-Davis 87] "GeoQL - A query language for geographic information systems," R. Sacks-Davis, K. McDonell, B. Ooi. Australian and NewZeland Association for the Advancement of Science Congress, Townsville Australia. 1987.

[Wiggins, French 91] "GIS: Assessing your Needs and Choosing a System," Lyna Wiggins, Steven French, AICP. In Planning Advisory Service, American Planning Association, 1991.