Map Hacking: On the use of inverse address-matching to discover individual identities from point-mapped information sources

Marc P Armstrong  
*University of Iowa*

Amy J Ruggles  
*University of Iowa*

**DOI:** [https://doi.org/10.17077/e2q3-g9p9](https://doi.org/10.17077/e2q3-g9p9)

Copyright © 1999 Marc P. Armstrong and Amy J. Ruggles

Hosted by Iowa Research Online. For more information please contact: lib-ir@uiowa.edu.
Map Hacking: On the Use of Inverse Address-Matching to Discover Individual Identities from Point-mapped Information Sources

Marc P. Armstrong & Amy J. Ruggles
Department of Geography
316 Jessup Hall
The University of Iowa
Iowa City, IA 52242
<firstname-lastname>@uiowa.edu

Abstract

The widespread availability of low-cost desktop GIS software now enables an unprecedented number of individuals to produce point-symbol maps from information considered confidential in its original, tabular, form. These maps, which are made by address-matching individual-level administrative records to street centerline files (e.g. TIGER) can be easily (and perhaps inadvertently) distributed in HTML format. These “raw” maps comprised of abstract map symbols do not directly disclose confidential information. However, a determined data spy can use GIS technology and other knowledge to “hack” the maps and make an estimate of the actual address (and hence, a good guess as the identity of an individual) associated with each point symbol. Though this process, called inverse address-matching, is supported by widely available GIS software, there has been almost no discussion in the GIS literature about factors that are important in successfully inverting the address-matching transformation. In this paper, we situate our work within current debates on privacy, and then conduct a set of controlled experiments that are designed to evaluate the performance of the address inversion process. We do this with the full understanding that such knowledge could be used for nefarious purposes. Such knowledge, however, can also be used to guard against individual-level identity disclosure by guiding the design and use of effective cartographic masking techniques.

1.0 Introduction and Background

In the United States and most of the developed world, privacy is often thought to be a fundamental right. Though not explicitly protected under the U.S. Constitution and Bill of Rights, privacy issues have figured prominently in subsequent legislation and are recognized explicitly in many other national constitutions and in the UN Declaration of Human Rights. Moreover, many nations and organizations are developing standards that concern access to personal information, (e.g. EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data - 95/46/EC and URLs 2, 6, 8,
9, 10). Despite its legislative prominence, however, privacy is difficult to define, since it is both contextual and contested [Goss, 1995:177, 2:5] and co-evolves with new technologies.\textsuperscript{1} Furthermore, the right to privacy is negotiated with personal values such as convenience and other fundamental rights, such as the right to a free flow of information and the right to personal security, other qualities thought of as public goods. In fact, we also may exchange (voluntarily or not) privacy for expediency and safety (e.g., unlisted numbers included in E-911).

Statutes stipulate that government agencies must collect and handle but usually not disseminate individual-level data. The Freedom of Information Act, for example compels the government to release certain types of information, but shields other types of information from public scrutiny (e.g., medical records) to maintain privacy. Privacy-ensuring policies and legislation reflect the growing public concern over the apparent erosion of privacy and the role of information technologies, notably the Internet, in society (Agre and Rothenberg, 1998, Rotenberg, 1999, and URLs 15:15, 2:3). Although the Internet has brought privacy concerns to the forefront of the public agenda, early concerns about the implications of computer data and processing date to the 1960s and 1970s. In 1973, a landmark U.S. publication (commissioned by Caspar Weinberger) described the scope of intrusions into the lives of U.S. citizens by computer-based technologies (U.S. Department of Health, Education and Welfare, 1973). This report was predated by data protection laws in Hesse, Germany (1970) and Sweden (1973). Legislation in the U.S. was passed in 1977. (URL 2:6)

As an information technology, GIS has a place in debates over privacy. Indeed, GIS technologies have a distinct role and characteristic abilities that may require special attention. A literature is emerging on the social implications of GIS (Craig and Elwood, 1998; Elwood and Leitner, 1998; Pickles, 1995; Sheppard, 1995), but only recently have researchers and theorists begun to elucidate specifically GIS-enabled threats to privacy (Barndt, 1998; Goodchild, 1999). While Goss (1995), for example, has examined privacy issues related to the collection and use of geo-demographic information in marketing, and Armstrong, Rushton and Zimmerman (1999) have evaluated alternative approaches to preserving the confidentiality of mapped medical information, empirical evidence that supports or refutes assertions made in the literature is absent. The purpose of this paper is to describe and evaluate how two characteristic GIS

\textsuperscript{1} In an evocative, although undoubtedly controversial phrase, the Economist described privacy as a "residual value" [15:15]
functions (1) mapping of address-matched data and (2) inverse address-matching of such data, can be combined to recover individual identities (and thus violate privacy) from data sources conventionally thought to be anonymous.

In current debates, there is often confusion between (or disparate definitions of) the terms "privacy", "confidentiality", and "anonymity" (URLs 1:13, 2:5). There is a general tendency to confuse privacy protection with efforts to keep personal information secure from unauthorized use. For example, most discussions about computer-based intrusions and the resulting policy implications (EU Directive, the US Safe Harbors, FGDC, UDHEW) are based upon generally similar principles\(^2\) that are designed to protect not so much privacy in the popular sense of anonymity, but upon data transparency, security, accuracy and a certain individual control over future applications, with at best limited options to opt out of certain databases (see also Goss, 1995:177, and URL 2:7). Anonymity (or de-personalization, the de-linking of personal data from its identifiable source) is usually only briefly mentioned in these documents, often as a precondition to certain forms of data-processing, or prior to the waiver of otherwise mandated safeguards (URLs 10:18; 7:2; 19:1; and EU Directive [recital 27, Article2(a), Article 8, paragraph 3]). The usual definition of anonymity as being reasonably secure from disclosure by both direct and indirect means (EU Directive, Article 2, Definition [a]) is important in a GIS context.

The research reported in this paper focuses on two related questions:

- With what level of accuracy can an address be recovered from a map?
- What types of errors occur and what is their impact on results?

The questions are addressed through the use of a controlled set of experiments. We begin with data sets that have known characteristics, create mapped representations of them and then attempt to hack these maps to recover the original information from them. In this way we can assess the success of the procedures used and then also examine for systematic errors in the inversion transformation. Such errors can occur for a variety of reasons related to data and the processes employed.

\(^2\) For example Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement in the proposed U.S. Safe Harbors standards.
2.0 Address Matching Factors

Address-matching (sometimes called geocoding) involves the transfer between files of an explicitly geographic descriptor of location to an implicitly geographic identifier. Though the result is often a single coordinate, the process can be extended to also include arcs, polygons, or raster cells, (e.g., a street, or house lot). Results can be specified not only as a street address, but also may include (or be) identifiers such as town, zip code, or zip+four code. This can be conceptualized as a two part process, (1) the identification of matching addresses in different files (essentially a specialized and complex database query) and (2) the transfer of the geographic information between files (a simple database activity). To this point, although address-matching is generally understood to be a characteristic GIS function (Dueker, 1974; Drummond, 1995), it requires only (sometimes enhanced) database functions. Such address-based joins are part of the role that GIS software plays in IT database convergence. However, it is when the addresses are mapped (perhaps only virtually), and the resulting geographic information is used to build relationships between otherwise incompatible databases, that the truly geographic contribution to IT database convergence emerges.

Inverse address-matching is a slightly different, but still characteristically and truly geographic contribution, in which mapped data, that appears to have lost the connection to whatever other personal information was contained in the database (and as a consequence is de-personalized), is transformed to recover the original addresses by digital means — map hacking. Map Hacking (a form of data spying) is an extreme form of recovering (personal?) information from maps. It describes situations in which one deciphers information, assumed to be private and/or secure, that has been coded stored in map form. The processes described below are generic techniques by which one can recover information from maps. Map hacking arises from the context in which such data-recover efforts occur.

The basic goal of map-hacking is the recovery of individual-level information from mapped data, specifically that mapped by an address-matching procedure (even more specifically in this research, arc-interpolated address-matching). A fundamental objective of much work in cartography has been an increase of positional accuracy (and decrease in spatial error). Because the mathematical processes (or transformations) of mapping can be mathematically reversed (or

---

3 Historically, geocoding could also involve the transfer of a different implicitly geographic identifier to a file. This ability is rarely discussed in the GIS literature, but continues to be of logical importance.
back-transformed), and the fundamental digital basemaps are of such positional accuracy, the
inverse transformations will likely recover the original mapped data subject to error limitations.
Even TIGER files, which were not originally designed to high levels of geometric fidelity, can
be used effectively to complete inversion tasks. Though additional advances in map-hacking can
be made by identifying the original pool of candidates, as well as through the use of other (non-
geographical) techniques to eliminate potential candidates, our focus is on geographic
techniques. While maps can be conceptually hacked with success, several practical impediments
to the process remain.

2.1 Offset
The results of an address-matching process are often mapped. Since topological information
is effectively removed when a map is produced, it must be reconstructed based purely on
geometrical relationships or some combination of geometry and logic. Thus when street
centerline files such as TIGER are used to provide the geometrical and topological information
needed to complete the address matching process, the resulting maps however are often modified
in a way that serves to “enhance” their realism. Offset is a way of introducing a displacement of
the symbol used to represent the address away from the street centerline. However, because of
this graphic transformation, when inverting the address-matching transformation points may be
incorrectly assigned to a road segment as a consequence of offset. This road-switching occurs
when the incorrect arc is returned in the reverse address matching process because of the relative
nearness of an address-matched location to two arcs. It is a fundamental error and must be
avoided if possible. In certain extreme cases, offset may result in symbols being placed inside an
adjacent block.

2.2 Squeeze

Because of the problems described above, the use of street centerline abstractions in address
matching may require the use of another parameter (squeeze) to ensure that address-based
symbols are located on their correct street segments. The use of squeeze means that symbols are
proportionally re-allocated along their street segment so that they are not placed closer to an
intersecting street segment. Obviously this problem would occur only for addresses that are
close to intersections, but a global (segment) transformation modifies symbol locations for all symbols on a given segment.

2.3 Hypothetical and actual address ranges

In some cases TIGER files contain address ranges that are incorrect. In many instances ranges are stored 100 per block when far fewer addresses actually exist. Thus for example, a street may have addresses that range from 1 to 39 along a block face and TIGER would report that the actual ranges are 1 to 99. In such cases a map for the 39 address produced from the spurious ranges would show that it was less than half way down the block (39/99), when in fact it is at the end of the block (39/39). In some cases the use of hypothetical addresses is not so much a mistake but may, instead, reflect planning reality rather than physical reality. The use of hypothetical ranges has the benefit that files are robust to changes in physical reality (e.g. splitting a lot into two parcels).

3.0 Methods

We began with a list of known addresses that were address-matched to a TIGER file to produce a map. The coordinates produced by this process were recovered and reduced to a text file. This file was then inverse address matched to obtain a list of addresses that were then compared to the original to determine the effectiveness of the process. In particular, data were obtained from the Iowa City Community School District and consists of administrative records (home addresses) for students enrolled in the district. Four sub-areas within Iowa City were chosen based on a priori evaluation of road network characteristics to include several different types (Table 1). Within each sub-area, we have a dataset of addresses known to match.

<table>
<thead>
<tr>
<th>Road network characteristics</th>
<th># addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: modern, curvy</td>
<td>156</td>
</tr>
<tr>
<td>B: grid, downtown</td>
<td>131</td>
</tr>
<tr>
<td>C: transitional</td>
<td>219</td>
</tr>
<tr>
<td>D: grid, residential</td>
<td>199</td>
</tr>
</tbody>
</table>
Offset
(Displacement away from street centerline)
Squeeze

(Proportional displacement caused by centerline representation)
For each sub-area address-matched maps were created using three different levels of offset and squeeze (Table 2). Using all combinations of these factors, we created nine address-matched maps for each of the four sub-areas: a total of 36 maps. From these we produced 36 files with only ID, Latitude and Longitude. These files were used in the reverse address matching process to produce "recovered addresses". Finally, these were compared to the list of known addresses and a "hit rate" was computed.

Table 2. Address-matching factors examined

<table>
<thead>
<tr>
<th>Offset (%)</th>
<th>Squeeze (m)</th>
<th>0</th>
<th>10</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An Arc/Info AML was written to invert the address-matches and obtain the required coordinates. Since we use address-matched coordinates exported by Arc/Info and then immediately inverse address-matched them, we have removed other sources of error that arise, for example, from digitizing and changing projection. Our experiment is designed to isolate the effects of offset and squeeze.

During reverse address-matching in Arc/Info, we were required to specify a search radius because that affected our success rate in a way that was especially noticeable at the larger offsets. The default search radius in Arc/Info is based on the bounding box of the layers, and comparisons between sub-areas. We set our search radius at Offset+1 (e.g. 1, 11, 21m) with the expectation that determining the offset of an address-matched map is a fairly trivial pre-processing step that can improve success rates.

Relational joins based on ID were made for our 36 tables, and we manually coded for correct matches. We used two criteria to evaluate the success of a reverse match:

- Exact correct address (strict), and
- Correct street only.
The second criterion allows us to assess the effect of squeeze on successful matches.

4.0 Results

The results we observed show a clear effect of both offset and squeeze on our ability to inverse the address matching transformation. This effect is manifest in inverting for both exact address and correct street only, though as expected the street-only results are impacted less severely. In table 3, which shows hit rates for exact address, we were able to correctly recover more than 95% of the addresses when offset or squeeze factors were not applied during address-matching. However, our hit rate plummeted, in some cases, to approximately 10% when an offset of 20 meters is combined with a 10% squeeze. Though this decrease was not uniformly observed the best results were only 30% for the maximum values of offset and squeeze that were used. Increases in the squeeze parameter reduced the number of exact hits the most in areas B and D, which are older grid-pattern areas with the greatest likelihood of incorrect address ranges. In three sub-areas (B, C, and D), the first increase in the value of the squeeze factor (from none to 5%) is proportionally greater than the effect from the second increase (from 5% to 10%).

Table 3. Success Rates for Exact Street Address

<table>
<thead>
<tr>
<th>Offset</th>
<th>Squeeze</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>93.59</td>
<td>95.42</td>
<td>91.78</td>
<td>93.97</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>46.15</td>
<td>22.90</td>
<td>43.38</td>
<td>27.64</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>25.64</td>
<td>8.40</td>
<td>29.22</td>
<td>11.56</td>
</tr>
<tr>
<td>10</td>
<td>None</td>
<td>83.33</td>
<td>81.68</td>
<td>77.17</td>
<td>72.36</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>42.95</td>
<td>20.61</td>
<td>37.90</td>
<td>23.12</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>23.08</td>
<td>6.87</td>
<td>24.66</td>
<td>12.06</td>
</tr>
<tr>
<td>20</td>
<td>None</td>
<td>71.79</td>
<td>67.18</td>
<td>63.93</td>
<td>56.28</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>40.38</td>
<td>19.85</td>
<td>32.42</td>
<td>23.12</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>22.44</td>
<td>6.87</td>
<td>20.09</td>
<td>10.05</td>
</tr>
</tbody>
</table>

Success rates are uniformly higher for correct street matches as expected (Table 4). In fact we were able to recover more than approximately 95% for all values of squeeze when offset was
equal to zero. This is an expected result since squeeze will not cause street switching and simply re-allocates addresses along the correct block face. In fact by increasing squeeze any errors arising from "street switching" are reduced (except for the anomaly in area C with offset = 10. The hit rate for the correct street only declines, however when offset is increased.
The differences in recovery rates still vary by subarea, but not as dramatically as measured by the correct address criteria of success. However, subarea A is less affected than the rest by increasing offset.
Table 4. Success Rates for Correct Street Only

<table>
<thead>
<tr>
<th>Offset</th>
<th>Squeeze</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>96.79</td>
<td>96.18</td>
<td>94.98</td>
<td>94.97</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>99.36</td>
<td>99.24</td>
<td>95.89</td>
<td>97.99</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>100.00</td>
<td>99.24</td>
<td>96.35</td>
<td>97.99</td>
</tr>
<tr>
<td>10</td>
<td>None</td>
<td>89.74</td>
<td>83.97</td>
<td>85.39</td>
<td>84.42</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>91.03</td>
<td>85.50</td>
<td>84.93</td>
<td>84.92</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>92.31</td>
<td>87.79</td>
<td>89.04</td>
<td>89.95</td>
</tr>
<tr>
<td>20</td>
<td>None</td>
<td>85.26</td>
<td>71.76</td>
<td>76.26</td>
<td>73.87</td>
</tr>
<tr>
<td></td>
<td>5%</td>
<td>87.82</td>
<td>74.05</td>
<td>77.17</td>
<td>76.88</td>
</tr>
<tr>
<td></td>
<td>10%</td>
<td>88.46</td>
<td>77.86</td>
<td>80.37</td>
<td>77.89</td>
</tr>
</tbody>
</table>

Because of the variability present among the different sub-areas we wished to examine each for the present of any systematic problems in the data sets. In some cases, we became suspicious of the address ranges present in the TIGER files. Consequently, for each arc we subtracted their low values from their high values. This was done for both sides of the street. As shown in Table 5 we observe a pronounced peak at (exactly) 100 for the "potential" ranges in each area. In the table, 0 means the address range is missing. Obviously, area B has the strongest peak at 100, followed by D, then C and A. A has the most missing address ranges, followed by C, then D, and B. In general, A and C have the most even distribution of ranges, probably indicating more actual addresses ranges. B and D are strongly peaked at 100, which indicates a tendency toward hypothetical ranges. Additional variables need to be investigated so that we can more completely understand the nature of error in the inverse address matching transformation (e.g. street intersection geometry).
Table 5. Distribution of address values for each street segment.

<table>
<thead>
<tr>
<th>X</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>20.64%</td>
<td>2.91%</td>
<td>18.93%</td>
<td>5.94%</td>
</tr>
<tr>
<td>0&lt;X&lt;100</td>
<td>31.70%</td>
<td>18.31%</td>
<td>27.80%</td>
<td>29.33%</td>
</tr>
<tr>
<td>100</td>
<td>40.00%</td>
<td>77.47%</td>
<td>48.83%</td>
<td>62.92%</td>
</tr>
<tr>
<td>100&lt;X</td>
<td>7.66%</td>
<td>1.31%</td>
<td>4.44%</td>
<td>1.81%</td>
</tr>
</tbody>
</table>

5.0 Discussion and Conclusions

In this paper we have demonstrated an ability to accurately recover a large proportion of original addresses from dot maps that were produced from our input data sets. We were able to recover the correct street for almost all of the input addresses and in some cases approximately 95% of the exact addresses. Several factors influenced the results. Increases in the amount of squeeze and offset used to create the dot maps from the raw addresses caused substantial reductions in our ability to recover addresses. In fact, at the maximum values for squeeze and offset we examined, our hit rate was reduced to less than 10% for exact address in some cases. There may also be large local address range “aberrations” in some areas. We observed this effect in older sections of our study area; there was a tendency toward “false” address ranges in which TIGER files contain, for example, 100 addresses for each block face irrespective of the observed ranges.

Other factors that we did not examine, however, also play a role in successful map hacking. Cartographic artifacts such as symbolism (e.g., large dots or small) and the level of generalization present on the map to be hacked will both play important roles. Small scale maps will, all things being equal, tend to be more difficult to hack than large scale maps.

With the addition of information about land use, easily obtained in some areas as ready-to-download layers, the overall accuracy of map hacking can be improved. When addresses fall into inappropriate areas based upon this ancillary data (such as recreational land-use polygons and lakes, for example) a reverse type of locational filter (used in the production of dot maps as shown by Dent, 1999:165) can be applied to reduce searching. This strategy may prove especially beneficial to the map hacker when addresses are randomly masked. Moreover, if a list of non-residential addresses is available, the choice set can be narrowed by eliminating such addresses from consideration. Like actual and hypothetical address ranges, such information can be obtained by mining digital phone directories or commercial directories.
These results should not imply that standard operations such as offset and squeeze are enough to protect privacy. These operations (especially offset) can themselves be back-transformed to improve accuracy. Furthermore, with the addition of information about land use, easily obtained in some areas as ready-to-download layers, the overall accuracy of map hacking can be improved. When addresses fall into inappropriate areas based upon this ancillary data (such as recreational land-use polygons and lakes, for example) a reverse type of locational filter (used in the production of dot maps as shown by Dent, 1999:165) can be applied to reduce searching.

Moreover, if a list of non-residential addresses is available, the choice set can be narrowed by eliminating such addresses from consideration. Such information can be obtained by mining digital phone or commercial directories. Integrating the inverse-address matching procedure with information obtainable from other IT databases will open still more possibilities for improved hit-rates. In fact, the GIS may only be used to produce pools of candidates (e.g., used to identify candidates on the correct block face - our "correct street category") and ancillary IT information, both geographic and non-geographic, will be used (perhaps involving statistical techniques) to reduce the pool of candidates.

Finally it is important to recall that mapping software is rapidly becoming ubiquitous. Databases getting larger and more accessible, and more people (often with no training in GIS or cartography) are making maps as a consequence. Address-matching and mapping capabilities have been spun-off GIS and are available independently on the Internet (for example, www.mapblast.com, www.mapquest.com). Certain forms of inverse address-matching are already available on the web (on the www.inforspace.com site) and it is likely that further cross-linking of GIS-related functions will occur.

6.0 References


Goss, J. 1995. We know who you are and we know where you live: The instrumental rationality of geodemographic systems. *Economic Geography* 71 (2): 171-198.


**URLs**

Safe Harbors: http://www.ita.doc.gov/ecom/menu.htm


May 12, 1999 Filed at 11:58 a.m. EDT
downloaded 5/12/1999

[4] Decoding developments in Iceland
   Bernhard Palsson and Snorri Thorgerisson Nature Biotechnology Vol 17 May 1999 page
   47
   PDF copy downloaded from http://biotech.nature.com May 13, 1999

   Nigel Duncan, British Medical Journal volume 318 April 1999 p. 1096
   PDF copy downloaded from http://www.gmj.com May 13, 1999

   Privacy in Federal Geospatial Databases (adopted by the Federal Geographic Data
   Committee in April 1998)

[7] Data Confidentiality and Security - it's YOUR Problem
   European Health Telematics Observatory [EHTO]
   Updated Sep 23, 1998
   Downloaded 5/12/1999

[8] Aaron Statement on Data Privacy and Electronic Commerce, Date March 15, 1999
   U.S. Department of Commerce
   Remarks of David L. Aaron - Under Secretary of Commerce for International Trade
   Before the Information Technology Association of America
   Fourth Annual IT Policy Summit
   The International Trace Center
   (Ronald Reagan Building) *BOO HISS!!*
   Washington, D.C.
   March 15, 1999

[9] With the show over, all eyes on NTIA as it prepares the Report
   Privacy Times, Vol 18, No 13, June 26, 1998
   http://www.privacytimes.com/ss-summit.html
   downloaded 5/13/1999

    www.ita.doc.gov/ecom/shprin.html
    Downloaded 5/13/1999

    Dee Ann Divis
    Geo Info Systems November 1998 pp 16-18

[12] Privacy for GIS Information: Part 2 of 2
    Dee Ann Divis
    Geo Info Systems January 1999 pp 18-20

[13] guest editorial Speaking with the enemy? A conversation with Michael Goodchild
    Environment and Planning D: Society and Space 1999 vol 17 pages 1-2

[15] The end of privacy
The Economist, May 1, 1999 page 15-16

[16] The end of privacy: The surveillance society
The Economist, May 1, 1999 pages 21-23

"We know who you are and we know where you live": The instrumental rationality of

[18] GAO/HEHS-99-55
February 1999

[19] The deCODE Proposal for an Icelandic Health Database
Ross Anderson
October 20, 1998
http://www.cl.com.ac.uk/users/rja14/iceland/iceland.html
Downloaded 5/17/99

Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal
Printing Office.


health data to preserve confidentiality. Statistics in Medicine, 18(5): 497-525.
