8-6-2009

Privacy and Geospatial Technologies

Lynn F. Brien
University of New Orleans

Privacy and Geospatial Technologies

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
In partial fulfillment of the
requirements for the degree of

Master of Arts
In
Geography

By

Lynn F. Brien

B.S. Louisiana State University, 1978

August, 2009

Dedication

This work is dedicated to my mother, Joycelyn Tobler Ferrara, who taught me to love learning.

Acknowledgement

I want to thank Dr. Mahtab Lodi for his inspiration and for his unwavering guidance, support, and patience. I would also like to thank the faculty of the Geography Department for their support and encouragement. Finally, I want to thank my beloved family for their enthusiastic support, without which this undertaking would have been difficult, if not impossible.

Table of Contents

Abstract

This research examines the role of geospatial and ancillary technologies in the erosion of privacy in contemporary society. The development of Remote Sensing, GIS, and GPS technologies are explored as a means of understanding both their current and predicted uses and capabilities. Examination is also made of the legal basis and current status of privacy rights in the United States. Finally, current and predicted uses and capabilities of geospatial and ancillary technologies are critically examined in light of existing privacy protections as a means of determining the ways in which these technologies are impacting privacy currently and what their effects may be in the future.

Keywords: geospatial technology, privacy, surveillance, law, technological development

Chapter 1

Introduction

1.1. Introduction

The assumption that the boundaries of privacy are shifting as a result of technological development is well documented (Armstrong and Ruggles, 2005; Dobson and Fisher, 2007; Curry, 1997; Haggerty and Ericson, 2000; Solove, 2008; O'Brien, 2008; Nissenbaum, 1998; Holtzman, 2006; Rosen, 2000). Geospatial and ancillary technologies, augmented by exponential increases in computing power and data storage capacity, appear to be playing a significant role. The trend towards integration of discrete technologies is expected to continue and to accelerate, yielding synergistic results. But how exactly are Remote Sensing, Geographic Information Science, and the Global Positioning System, along with ancillary technologies, contributing to shifts in privacy boundaries?

Because geospatial technologies are firmly rooted in the discipline of geography, having been developed on the most basic of geographic principles, and because they play a central role in the modern practice of geography and geographic research, it is essential that geographers contemplate this question.

1.2. Purpose

The purpose of this research is to examine the role of geospatial and ancillary technologies in the erosion of privacy in contemporary society. This is accomplished by first tracing the development of individual technologies in an attempt to clearly understand both current and predicted uses and capabilities. Second, an examination is made of the legal basis and current status of privacy rights in the United States. Third, current and predicted uses of geospatial and ancillary technologies are critically examined in light of existing privacy protections in an effort to answer the central questions of this thesis: Are geospatial and ancillary technologies impacting and ultimately compromising privacy, and, if so, to what extent? And what will likely be their future role relative to privacy?

1.3. Methodology

This research is based on an in-depth review of available literature on remote sensing technology, geographic information systems (GIS), global positioning system (GPS), and ancillary technologies. The history and development of geospatial technologies, as well as their current and predicted future applications, were thoroughly investigated. Furthermore, legal, ethical, and theoretical aspects of public privacy issues were examined in detail.

1.4. Structure

Chapter 2 traces the history and development of Remote Sensing, with particular emphasis on the Landsat program and the transition from military to civilian to international commercial applications of space remote sensing, culminating in a discussion of predicted future applications. Chapter 3 outlines the history and development of Geographic Information Science and Systems, briefly describing the major players and innovations, and ending with a discussion of present and predicted future applications. Chapter 4 describes the Global Positioning System, its history and development, and briefly discusses emerging global navigation satellite systems. Chapter 5 discusses privacy concepts and theories and outlines the legal basis for privacy rights in the United States, with a brief description of discrepancies between privacy protection in the European Union and the US. Chapter 6 discusses many of the current and predicted uses of geospatial and ancillary technologies and their impact on privacy, particularly in the United States. Chapter 7 discusses the conclusions and implications of the research findings.

1.5. Endnotes

ARMSTRONG, M., RUGGLES, A. J., 2005, Geographic information technologies and personal privacy. *Cartographica,* 40: 63-73.

CURRY, M. R., 1997, Digital People, Digital Places: Rethinking Privacy in a World of Geographic Information. *Ethics & Behavior*, 7: 253-264.

CURRY, M. R., 1997, The digital individual and the private realm. *Annals of the Association of American Geographers*, 87: 681-699.

DOBSON, J. E., FISHER, P. F., 2007, The Panopticon's Changing Geography. *Geographical Review,* 97: 307-323.

HAGGERTY, K. D., ERICSON, R. V., 2000, The surveillant assemblage. *British Journal of Sociology,* 51: 605-622.

HOLTZMAN, D. H., 2006, *Privacy Lost: How Technology is Endangering Your Privacy.* Jossey-Bass, San Francisco, pp. 8, 31, 93-117, 176-178.

NISSENBAUM, H., 1998, Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17: 559-596.

O'BRIEN, M., 2008, Law, privacy and information technology: a sleepwalk through the surveillance society? *Information and Communications Technology Law,* 17: 25-35.

ROSEN, J., 2000, *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, New York, pp. 8, 10, 12, 20, 216-217, 219, 169-170.

SOLOVE, D. J., 2007, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review,* 44: 745-772.

Chapter 2

Remote Sensing

2.1. Defining Remote Sensing

The American Society for Photogrammetry and Remote Sensing (ASPRS) defines remote sensing as "the art, science, and technology of obtaining reliable information about physical objects and the environment, through the process of recording, measuring and interpreting imagery and digital representations of energy patterns derived from non-contact sensor systems" (ASPRS, 1988). Remote sensing is more generally understood as the acquisition of information about the earth from a distance by recording electromagnetic radiation (EMR) reflected or emitted from the Earth's surface features. Once recorded, the information is processed, analyzed and applied to enrich our understanding of the earth's surface features, both cultural and physical, and the processes affecting those features. Remote sensing is an art as well as a science because analysis of remotely sensed data often requires mathematical algorithms and automated processing, as well as human interpretation based on the observations, experience, and creative problem solving skills of the analyst.

Despite its most frequent association with satellite imagery and aerial photography, remote sensing, in its broadest sense, encompasses any collection of data accomplished at a distance from the source. Defined in this way, remote sensing is a ubiquitous part of modern life, accomplished through the use of many different kinds of devices, including, but not limited to cameras, audio recording devices, etc. These devices are considered 'passive' when they require an external energy source to collect data, or 'active' when they provide their own source of energy. For instance, an ordinary camera is an example of a 'passive sensor', whereas traffic radar is an example of an 'active sensor'.

In its narrowest context, remote sensing is based on sensors which reside on platforms that are always some distance from the target and which may be located on the ground, on an aircraft, or on a spacecraft or satellite. Ground based sensors are generally capable of acquiring more detailed spatial and spectral information about earth's cultural and physical features, as compared with remotely sensed data acquired from sensors on board aircraft or space borne satellites. In the broadest context, remote sensors may reside nearly anywhere and may be hidden and/or invisible or nearly invisible to the human eye.

2.2. The History of Remote Sensing

2.2.1. Aviation and Aerial Photography

The dual histories of photography and aviation provide the basis for the history of remote sensing. Remote sensing can be traced to Napoleonic times and the military use of hot-air balloons to observe and assess enemy strength and position (Shekhar and Xiong, 2008). As early as 1794, French aeronauts stationed in tethered balloons used telescopes to obtain information and produce sketches and annotated maps for use in military planning (Monmonier, 2002). While the daguerreotype made ground based image production practical in the 1850s, long exposure times proved prohibitive for aerial military surveillance. Still, the first known aerial photograph was taken in Paris in 1858 by Gaspard-Felix Tournachon, who was also known as "Nadar" (Lillesand et. al., 2008). James Wallace Black is credited with taking the earliest surviving aerial photograph over Boston in 1860 (Lillesand et. al., 2008).

Beginning around 1882, kites were used to obtain aerial photographs. Perhaps most famously, American G.R. Lawrence used kite photography to obtain images of San Francisco following the great earthquake and fires of 1906 (Lillesand et. al., 2008). Less well known are photographs resulting from experiments using carrier pigeons as platforms for 7 gram cameras (Lecture, EES 4093G, 2008).

The airplane was first used as a camera platform in 1908 when aerial motion pictures were taken over France by a photographer accompanying Wilbur Wright (Lillesand et. al., 2008). The use of aircraft as a platform for photography-based military reconnaissance became common during World War I, with over a million aerial photos collected for that purpose (Lillesand et. al., 2008). World War II saw the introduction on military aircraft of a rigid frame holding 3 cameras, one pointing directly down and the others pointing left and right, resulting in a series of 3 slightly overlapping, simultaneously captured photos, automatically taken at constant intervals. Flying charts depicting 16 million square miles were produced by the US Army Air Force during the 1940s using this technology (Monmonier, 2002).

2.2.2. Space-based Remote Sensing

A rocket propelled camera system, designed for retrieval by parachute, was patented by Ludwig Rahrmann in Germany in 1891 and marks the beginning of space remote sensing. Soon gyrostabilization was incorporated by German Alfred Maul, who by 1912 succeeded in launching camera apparatus weighing 41 kilograms to a height of 790 meters (Lillesand et. al., 2008). A period of rapid advancement of space remote sensing began around 1946, with US military testing of photographic capabilities using rockets, ballistic missiles, early satellites and manned spacecraft, all of which methods produced crude images but underscored the potential value of the technology (Lillesand et. al., 2008).

By 1960, TIROS-1, the first Television and Infrared Observation Satellite was launched. While its coarse images captured cloud patterns, this early weather satellite provided an indistinct view of the earth's surface. Advancements in sensor technology led eventually to better views of both the earth's atmosphere and its surface (Lillesand et. al., 2008).

2.2.3. Military Space Imaging

Also in 1960, with the Cold War underway, the US Department of Defense launched its first successful military reconnaissance satellite under the cover name Discoverer-14, purportedly for space research. In a single day of orbit, the "deep black", i.e. top-secret, Corona satellite collected more imagery of Soviet territory than had been collected during the previous four years using single pilot U-2 spy planes (Monmonier, 2002).

In contrast to modern satellites which transmit data electronically, the early Corona satellites were “giant disposable cameras” snagged mid-air as they re-entered the earth’s atmosphere (Monmonier, 2002). In operation from 1960 through 1972, Corona satellites were placed in near-polar elliptical orbits which varied in altitude from more than 800 kilometers to less than 180 kilometers, allowing for varying resolution. The first Corona camera system, KH-1 (Keyhole being the government’s name for top-secret satellite reconnaissance), mimicked 12 meter resolution when its orbit brought it closest to earth. By 1963, the National Reconnaissance Office (NRO), established to manage satellite spying, launched Corona satellites with KH-5 and KH-6 camera systems capable of 2 meter resolution when orbiting at lowest altitudes, with missions lengthened to 23 days. By 1966, KH-7 and KH-8 systems refined resolution to a mere 15 centimeters (6 inches) at lowest altitudes, with missions extended to 6 months or longer (Monmonier, 2002).

1971 brought the launch of KH-11, Corona’s first digital multispectral imaging system which incorporated newly invented light sensitive semiconductors (CCDs). Thus unburdened by film or recovery capsules, the new Corona satellites were now capable of multi-year missions. Off nadir imaging capabilities allowed once-a-day coverage for any area in the world. Sun-synchronous orbits of two KH-11 satellites allowed for multiple passes over areas deemed sensitive by intelligence agencies (Monmonier, 2002).

While details of early Corona satellites were declassified in 1995, information on later satellite capabilities is more speculative (Lillesand et. al., 2008). The Hubble Space Telescope is widely believed to be “an unclassified version of the KH-12” launched in 1986 with estimated 10 centimeter (3.9 inch) resolution (Monmonier, 2002).

2.2.4. Civilian Remote Sensing: A Brief History of The Landsat Program

Because of the classified status of the NRO satellite programs, remote sensing was essentially unknown to the civilian population except through the Mercury, Gemini, and Apollo manned space programs of the 1960s. The success of these programs in collecting photographic imagery for earth resource applications illustrated the value and significance of space remote sensing for monitoring earth resources and paved the way to the systematic acquisition of earth surface imagery on a regular basis (Lillesand et. al., 2008).

Understanding the history of remote sensing requires understanding the distinction between government owned public sector civilian observation satellites and privately owned commercial observation satellites. Until recently, civilian remote sensing has been dominated by the US, both with regard to remote sensing technology and remote sensing policy.

The first civilian remote sensing satellite, which was part of the Landsat series, was developed by the National Aeronautics and Space Administration (NASA) under the Earth Resource Technology Satellite (ERTS) program. Launched in 1972, Landsat 1 provided the first remotely sensed satellite images of the earth available for purchase by the nongovernmental sector. The use of Landsat 1's multispectral imagery was generally limited to scientists, academia, and government agencies, as the coarse 80 meter resolution was of limited value commercially (Florini and Dehqanzada, 1999). Landsats 2 and 3, launched in 1975 and 1978 respectively, were slightly updated versions of Landsat 1. Concurrently, NASA was also developing the Thematic Mapper (TM) with planned 30 meter resolution for incorporation into future Landsats 4 and 5 (Williamson, 1997).

In 1979, in an effort to encourage the use of Landsat data, the Carter administration issued Presidential Decision Directive 54 (Florini and Dehqanzada, 1999). As a result, the Landsat program was transferred from NASA to the National Oceanic and Atmospheric Administration (NOAA), under the direction of the US Department of Commerce. The intention was to foster an environment encouraging commercialization of the civilian remote sensing industry by creating opportunities for expansion within the private sector. The administration reasoned that future 30 meter resolution to be ushered in by Landsats 4 and 5 in the next half decade, along with cost declines accompanying commercialization, would help create a viable market in the private sector, as well as within the government, for commercial remote sensing data (Williamson, 1997; Florini and Dehqanzada, 1999).

Unlike the carefully paced transition envisioned by the Carter administration, the Reagan administration, in an effort to cut federal spending, advocated a swift acceleration of the process, the plan for which, in retrospect, has been called “ambitious but flawed” (Florini and Dehqanzada, 1999; Williamson, 1997). Between 1982 and 1983 feasibility studies commissioned by the US government were conducted by the Civil Operational Remote Sensing Satellite Advisory Committee (CORSSAC) of the Department of Commerce, by the National Academy of Public Administration, and by private entities, ECON Incorporated and Earth Satellite Corporation, with unanimous results. The plan to transfer Landsat to the private sector was characterized as “forced premature privatization….” wherein “No option was found that would permit the [Landsat] program to be commercialized, today or in the near future, without substantial subsidies or government-guaranteed data purchases” (Florini and Dehqanzada, 1999). The administration ignored all four reports recommending gradual commercialization and advising that the commercial market was not yet viable (Florini and Dehqanzada, 1999).

Particularly controversial was the Reagan administration’s plan to transfer weather satellites to the private sector. Opponents argued that the data constituted “public goods” to be retained in the public sector. The plan failed due in large part to negative domestic and worldwide reaction to the prospect of the sale, rather than the free exchange, of weather data (Williamson, 1997).

The Reagan administration’s federal spending cuts necessitated Congressional action to provide funding and save the Landsat program. In 1984, Congress passed the Land Remote Sensing Commercialization Act, which provided continued funding. The legislation also required the selection of a private contractor to administer the program and called for nondiscriminatory marketing of Landsat data, as well as archiving of the data. Additionally, it established a licensing process for the newly commercialized remote sensing industry (Florini and Dehqanzada, 1999; Hoversten, 2001). Maintaining continuity of data and controlling cost were important factors in the debate surrounding privatization and its implementation. Users of remotely sensed data required assurance of the availability of compatible data products in order to justify investments of research funds (Williamson, 1997).

In 1985 Earth Observation Satellite Company (EOSAT), a joint venture of RCA Corporation and Hughes Aircraft Company, was chosen by NOAA to take over the Landsat program and to market data products under a 10 year contract. The agreement included government subsidies to offset the undeveloped market. The subsidies were later cut by the Reagan administration, once again requiring Congressional action to save the program (Florini and Dehqanzada, 1999).

The early history of the Landsat program is marked by continuing and persistent budget crises. In 1989 with Landsats 4 and 5 functioning beyond their predicted life spans, NOAA planned to have EOSAT turn off the satellites for lack of funds. The outcry domestically and abroad resulted in a funding plan to save the program, a recommendation by the National Space Council to keep the program running since it was the only source of civilian remote sensing data, and the reversal of NOAA's plan to turn off the satellite (Florini and Dehqanzada, 1999). However, the chronic budget problems undermined market confidence in the future continuity and availability of data, thereby slowing the industry's growth (Williamson, 1997).

Despite the 1989 approval by the Bush administration to continue funding Landsats 4 and 5 and to launch the new Landsat 6, the program again faced budget crises in 1990 and 1991, causing the government to re-evaluate the Land Remote Sensing Commercialization Act of 1984. It was obvious the commercialization effort had failed. The effort had resulted in higher than anticipated government costs. Additionally, the cost to consumers had increased significantly, causing a drop in demand. With single thematic mapper scenes priced at $4,400, sales of imagery decreased from 35,272 images in 1984 to 8,000 in 1990 (Florini and Dehqanzada, 1999).

In 1986 French Systeme Pour l'Observation de la Terre, (SPOT) launched SPOT-1, which emerged as Landsat's first viable competitor, with 10 meter spatial resolution imagery and shorter revisit times. By 1987, the former Soviet Union made 5 meter resolution imagery commercially available and by 1989 SPOT's sales surpassed EOSAT's, suggesting that the US was quickly losing dominance. These developments further underscored the failure of the commercialization effort (Florini and Dehqanzada, 1999).

Finally, growing recognition of the invaluable role played by Landsat imagery in the 1990-91 Persian Gulf War helped to force a reevaluation of the commercialization effort. Estimates of Landsat imagery expenditures by the US Department of Defense (DoD) during the war range between $5 and $6 million (Florini and Dehqanzada, 1999).

As a result of these pressures, the Land Remote Sensing Policy Act was passed by Congress in 1992. The legislation terminated the commercialization efforts and placed the program under the management of NASA and DoD, acknowledging that, "the continuous collection and utilization of land remote sensing data from space are of major benefit in studying and understanding human impacts on the global environment, in managing the Earth's natural resources, in carrying out national security functions, and in planning and conducting many other activities of scientific, economic, and social importance" (Williamson, 1997; Florini and Dehqanzada, 1999).

Disagreements between DoD and NASA emerged in 1993 regarding budgeting for Landsat 7 and the types of sensors to be incorporated into the satellite. During this time Landsat 6 failed to launch, making the launch schedule and budget considerations of Landsat 7 more critical and resulting in the DoD's resignation from the program. DoD prefered incorporating the 5 meter resolution High Resolution Multispectral Stereo Imager (HRMSI), but NASA wanted instead to use the Enhanced Thematic Mapper Plus (Williamson, 1997; Florini and Dehqanzada, 1999).

The Clinton administration's 1994 Policy on Foreign Access to Remote Sensing Capabilities (Presidential Decision Directive 23) placed responsibility for the development and launch of Landsat 7 on NASA, with responsibility for the operation of the spacecraft given to NOAA. The Department of the Interior was given responsibility for the archiving and distribution of Landsat 7 data. Most significantly, the data was to be distributed "at the marginal cost of reproduction" (Florini and Dehqanzada, 1999).

NASA's Mission to Planet Earth (MTPE) emerged around this time, with the goal of understanding "the total Earth system and the effects of natural and human-induced changes on the global environment" (NASA Mission to Planet Earth, 2009). Later known as Earth Science Enterprise, the program is currently called the Earth-Sun System Missions (Lillesand et. al., 2008). Launched in 1999, Landsat 7 is managed by NASA, with data collected and distributed by the United States Geological Survey (USGS) of the US Department of the Interior. It was designed to provide 30 meter multispectral and 15 meter panchromatic imagery at minimal cost described as "the cost of fulfilling user requests" (Florini and Dehqanzada, 1999).

In order to insure continuous coverage, a plan was made in 2004 to place sensors comparable to Landsat 7's on board the National Polar-Orbiting Operational Environmental Satellite System (NPOESS). However, in 2005, that plan was replaced by the Landsat Data Continuity Mission's (LDCM) plan to launch the Operational Land Imager (OLI) in July, 2011. The OLI will offer 12-bit 30 meter resolution for visible through shortwave infrared (SWIR) and 15 meter panchromatic data in visible regions of the electromagnetic spectrum. It will have 9 spectral bands with mid-morning equatorial crossing and a 16 day repeat cycle (NASA Landsat Data Continuity Mission, 2009). The plan is to calibrate OLI data with previous Landsat data and to offer orthorectified data products free via the web within 24 hours of capture (NASA Landsat Data Continuity Mission, 2009).

2.2.5. The Development of US and International Commercial Remote Sensing

Despite the establishment of licensing and regulation guidelines for the US commercial remote sensing industry by the Land Remote Sensing Commercialization Act of 1984, nearly a decade passed before a private remote sensing firm emerged (Florini and Dehqanzada, 1999). However, following the Land Remote Sensing Policy Act of 1992, WorldView, Inc. received licensing for the EarlyBird, a system characterized by minimal instrument and launch costs. WorldView's marketing plan, based on commercial objectives, was to service the information industry quickly and efficiently through the internet and related information technologies (Williamson, 1997). The explosive growth which followed Earlybird's debut is attributed to both political and technical developments.

The collapse of the Soviet Union removed barriers to the marketing of imagery. Prior to this event, dual-use technologies (with both civilian and military applications) were closely scrutinized by the US government, resulting in the discouragement of private investment (Florini and Dehqanzada, 1999). Additionally, growing confidence in the potential for exponential growth of demand for remote sensing imagery encouraged investment. Investors recognized that the market for satellite data products is vast, with those products having agricultural, urban planning, environmental, emergency response, media, and geological applications, among others, in addition to military and intelligence applications (Florini and Dehqanzada, 1999). It was noted in 1997 that, "A key component of the evolution from programs centered on supporting government needs to private sector initiatives is the growing understanding that land remote sensing could have a significant role in the rapidly expanding information marketplace" (Williamson, 1997). Coupled with growing recognition of market potential, the technological advances in data acquisition, storage and processing, the advances in personal computing, the development of GIS and RS software, and the emergence of the internet, all contributed to the growth of the commercial satellite industry (Florini and Dehqanzada, 1999; Williamson, 1997).

The government's role in the development of commercial remote sensing has been crucial. Along with Clinton's 1994 Presidential Decision Directive softening restrictions on the sale of high resolution satellite imagery to foreign entities, direct subsidies to private companies and guaranteed data purchases by the government have also contributed to growth. The US intelligence community continues to routinely contract with private companies for the purchase of high resolution imagery (Florini and Dehqanzada, 1999).

Since the late 1980s additional competitors to the US remote sensing industry have emerged, including the Indian National Remote Sensing Agency, the European Space Agency (ESA), the Japan Space Development Agency, and the Canadian Aeronautics and Space Institute. As of 2008, approximately 30 governmental and commercial satellite systems are operating in the optical spectrum. Countries having launched moderate resolution systems (4-60 meter resolution) include Algeria, Turkey, Nigeria, UK, China, Brazil, Thailand, and Korea. Other countries with moderate resolution systems being planned, developed, or operated include Germany, Singapore, South Africa, Vietnam and Israel. By 2010, countries with high resolution satellites (sub-4 meter resolution) will include the US, Israel, France, Russia, Korea, India, Taiwan, Thailand, UK, Japan, and Malaysia. The US, Israel, and France have, or will have by 2010, commercial satellite systems operating at sub-1 meter panchromatic resolution. Additionally, both the US and the European Space Agency currently have satellite systems with hyperspectral scanning capabilities, with Germany, India, Canada, and Italy currently developing hyperspectral systems (Lillesand et. al., 2008).

2.3. The Future of Space-based Remote Sensing

Space remote sensing's expanding scientific, economic, and social influence is international in scale and parallels increasing technological capabilities. The development of space remote sensing is away from large monolithic instrument laden satellites towards groups of collaboratively functioning relatively low cost miniature satellites (Bae, 2006). Among the smallest satellites are nanosatellites weighing 1 to 10 kilograms and picosatellites weighing 0.1 to 1 kilogram, made possible through technological advancements in power generation and electronics packaging, along with the development of micro-electro-mechanical systems (MEMS) and the functional integration of spacecraft structures (Arslan et. al., 2006; Das and Cobb, 1998).

The movement away from the placement of multiple scientific instruments aboard large expensive platforms means improved economic feasibility, reduced risk, and more efficient operation. This trend allows for mass production, economies of scale, and not least, the synergism resulting from formation flying of multiple mini-satellites (Das and Cobb, 1998; Delin and Jackson, 2001). Miniature satellites provide flexibility in launching as well as in operation. The clustering of mini-satellites, each of which is autonomous, collaborative, and reconfigurable, also allows for individual replacement or update of failing or outdated member satellites without risk to the system as a whole (Prescott et. al., 1999).

NASA's Earth Science Vision Initiative embodies the concept for the next generation of Earth Observing System satellites, the functions of which will be coupled with airborne and in-situ sensors as well (Prescott et. al., 1999). NASA's goal is to launch fleets of intelligent satellites which are both adjustable and self-adjusting, based on changing mission requirements. The idea is to move beyond distributed sensors or sensor networks, both of which merely collect and transmit data, to Sensor Webs consisting of spatially distributed sensors, with those aboard mini-satellites forming in aggregate a "virtual satellite" with coherent large apertures for data collection (Das and Cobb, 1998; Bae, 2006). Sensor Webs go far beyond the collection and transmission of data, possessing the capacity to share data omni-directionally among the member satellites and modify their functions in response to that data. As such, they have been characterized as "capable of automated reasoning" and able to "perform intelligent autonomous operations in uncertain environments…" (Delin and Jackson, 2001). The capacity for member reconfiguration means that Sensor Webs can more quickly and efficiently respond to unusual events, allowing for multiple angle, multiple sensor, multiple resolution and multiple spectral observations of those events, thereby underscoring the value of Sensor Webs in Earth observation and other applications (Zhou and Katafos, 2002).

The Jet Propulsion Laboratory's (JPL's) Sensor Webs Project was formulated to meet NASA's Earth Science Vision Initiative goals (Delin and Jackson, 2001). As of 2001, the project had documented success in building and operating instruments demonstrating Sensor Web concepts in the field (Delin and Jackson, 2001). It is predicted that, "the Sensor Web will become a ubiquitous instrument in the future, particular in applications that require an intelligent, virtual presence" (Delin and Jackson, 2001).

2.4. Endnotes

AMERICAN SOCIETY FOR PHOTOGRAMMETRY AND REMOTE SENSING (ASPRS), 1988, in *Introductory Digital Image Processing,* Jensen, J. R., 2005, Pearson Prentice Hall: Upper Saddle River, NJ, p. 3.

ARSLAN, T., HARIDAS, N., YANG, E., ERDOGAN, A. T., BARTON, N., WALTON, A. J., THOMPSON, J. S., STOICA, A., VLADIMIROVA, T., MCDONALD-MAIER, K. D., HOWELLS, W.G. J., 2006, ESPACENET: A Framework of Evolvable and Reconfigurable Sensor Networks for Aerospace – Based Monitoring and Diagonistics. *Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems* (AHS'06).

BAE, Y. K., 2006, A Contamination-Free Ultrahigh Precision Formation Flying Method for Micro-, Nano-, and Pico-Satellites with Nanometer Accuracy. *Space Technology and Applications International Forum, American Institute of Physics,* pp. 1213-1223.

DAS, A., COBB, R., 1998, TechSat 21 – Space Missions Using Collaborating Constellations of Satellites. *12th AIAA/USU Conference on Small Satellites*.

DELIN , K. A., JACKSON, S. P., 2001, The Sensor Web: A New Instrument Concept. *Presented at SPIE's Symposium on Integrated Optics*, 20-26 January, San Jose, CA.

FLORINI, A. M., DEHQANZADA, Y. A., 1999, No More Secrets?: Policy Implications of Commercial Remote Sensing Satellites. Publisher: *Carnegie*, Carnegie Paper No. 1, July 1999.

HOVERSTEN, M. R., 2001, US National Security and Government Regulation of Commercial Remote Sensing From Outer Space. *The Air Force Law Review*, 50: 253-280.

LECTURE, University of New Orleans, EES 4096G, October 6, 2008.

LILLESAND, T. M., KIEFER, R. W., CHIPMAN, J. W., 2008, *Remote Sensing and Image Interpretation*, *6th Edition*, John Wiley & Sons, Hoboken, NJ, pp. 42-45, 59-61, 401-403, 471.

MONMONIER, M., 2002, *Spying with maps.* The University of Chicago Press, Chicago, pp. 12-15, 18-19, 22-30.

NASA LANDSAT DATA CONTINUITY MISSION, [http://ldcm.nasa.gov/procurement/OLI-RD_061102R.pdf], accessed April 13, 2009.

NASA MISSION TO PLANET EARTH, [http://www.hq.nasa.gov/office/nsp/mtpe.htm], accessed April 13, 2009.

PRESCOTT G. E., SMITH, S. A., MOE, K., 1999, Real-Time Information System Technology Challenges for NASA's Earth Science Enterprise. *Proceedings of the 20th IEEE Real-Time Systems Symposium, 1999*.

SHEKHAR, S., XIONG, H., Eds., 2008, *Enyclopedia of GIS*. Springer, New York, p. 291.

WILLIAMSON, R. A., 1997, The Landsat Legacy: Remote Sensing Policy and the Development of Commercial Remote Sensing. *Photogrammetric Engineering and Remote Sensing*, 63: 877-885.

ZHOU, G., KATAFOS, M., 2002, Future Intelligent Earth Observing Satellites. *Pecora 15/Land Satellite Information IV/ISPRS Commission I/FIEOS 2002 Conference Proceedings.*

Chapter 3

Geographic Information Systems and Science

3.1. Geographic Information Systems and Science Defined

Geographic Information Systems are generally thought to encompass the acquisition, storage, analysis, and dissemination of geographically referenced data. A distinction is made between Geographic Information Systems (GIS) and Geographic Information Science (GISci), with the latter considered “the science of spatial data processing” or “the science behind the systems” (Kemp, 2008; Bossler et. al., 2001). GIS is concerned with hardware and software, combining database management systems with graphics capabilities (Bossler et. al., 2001). In contrast, GISci is concerned with the theory underlying the development and application of geographic information systems, including “database theory, methods of analysis, and visualization techniques” (Korte, 2001). Other terms considered synonymous with Geographic Information Science include Geocomputation, GeoInformatics, and GeoProcessing. (Wilson and Fotheringham, 2008). GIS and GISci have become nearly indispensible in research areas as diverse as Earth science and human health, as well as in practical applications, including communication and transportation networking and resource management (Goodchild, 2008).

3.2. The History of GIS and GISci

There exist early cartographic models dating back centuries, which can correctly be identified as Geographic Information Systems, albeit primitive ones by modern standards. In addition to the often cited example of Dr. John Snow’s 1854 mapping of cholera deaths in London, French cartographer Louis-Alexandre Berthier’s maps of the American Revolution’s Battle of Yorktown included hinged overlays portraying troop movements. Another example is the mid-19th century “Atlas to Accompany the Second Report of the Irish Railway Commissioners,” which layered geology, topography, population, and traffic flow on a single base map (University of British Columbia, Department of Geography, 2008). In each instance, the mapping product embodies the core concept of GIS by incorporating layers of data superimposed on base maps. This layering allows for the integration of autonomous data sets based on geography, while also pairing images with associated attribute information. While the history of GIS may therefore be longer and richer than it first appears, modern computer-based GIS as we know it today, dates back mere decades.

The remarkable evolution of GIS is characterized by a convergence of technological advances, ecological awareness, public support, and private enterprise. Key markers include, but are not limited to, developments associated with the following: the Canada Geographic Information System; the Harvard Laboratory for Computer Graphics and Spatial Analysis; the Experimental Cartography Unit, UK; the US Bureau of the Census; the Minnesota Land Management Information System; Triangular Irregular Networks; and advances in commercial software, particularly by Environmental Systems Research Institute (ESRI), Earth Resources Data Analysis Systems (ERDAS), Intergraph Corporation, and more recently by IDRISI (GIS History Project, 2008; Kemp, 2008). Additionally, of primary significance are developments driven by US Department of Defense sponsored research, including aerial and space based remote sensing technologies, the Global Navigation Satellite System (GNSS) and the Global Positioning System (GPS), all of which have been essential to the development of modern GIS.

A study of the history and development of GIS makes clear that the innovation that is computerized GIS uses spatial analysis techniques original to the discipline of Geography. While GIS has far reaching, some would say universal, applications, at its core is the study of place, making Geography its primary domain.

3.2.1. Canada Geographic Information System

The Canada Geographic Information System (CGIS) is considered the earliest operating GIS. It was developed in the 1960s as the basis for a land resource survey project called the Canada Land Inventory. The objective of the project was the comprehensive nationwide mapping of land use suitability, including existing land use, in order to provide a tool for planning and conflict resolution. CGIS, a joint project of the Canadian government and the private sector, was developed under the guidance of Roger Tomlinson, generally regarded as the "father of GIS". Over the course of 10 years, 2.6 million square kilometers were mapped (Kemp, 2008; University of British Columbia, Department of Geography, 2008). The sheer magnitude of the data required a state of the art mainframe computing system developed by IBM specifically for the project. Because the primary focus of the CGIS was spatial analysis rather than computerized cartography, overlay capabilities for 8 or more maps were designed specifically for the integration of varied information, such as environmental and socioeconomic data. Due to the geographical scope of the mapping project, innovative map linking techniques were created, as was the first optical drum scanner for map digitizing. Based on a vector approach using point, line, and polygon data, CGIS allowed for the analysis of databases consisting of over 500,000 polygons, a remarkable capability at that time (Kemp, 2008; University of British Columbia, Department of Geography, 2008). Additionally, the use of data frames within the vector approach was critical to the analysis of that magnitude of data, as it was a means of breaking the analysis into subsets. The CGIS was fully operational until 1994, a lifespan of approximately 30 years. Its impact on concepts and capabilities in resource management, environmental impact assessment, and sustainable development, and the field of geography in general, are immeasurable (Kemp, 2008; University of British Columbia, Department of Geography, 2008).

3.2.2. The Harvard Laboratory

The Harvard Laboratory for Computer Graphics and Spatial Analysis, part of the Graduate School of Design at Harvard University, was founded by Chicago architect, Howard Fisher with a 1965 Ford Foundation Grant awarded for his prototype of the SYMAP software (Kemp, 2008). Further developed by a team of programmers, the software featured attributes associated with points, lines and polygons, and could produce contour or choropleth maps. Distributed to institutions throughout the US, the software was a relatively inexpensive simple to use mapping package. SYMVU soon followed, allowing 3-dimensional display. Later, CALFORM accommodated plotter printing and POLYVRT allowed for conversion to cartographic databases (Kemp, 2008). Other topics of research included techniques for environmental planning and grid analyses software. Commercial distribution of Harvard's ODYSSEY software package, which focused on topological data, was considered but not pursued. Additionally, research at Harvard Laboratory on cartographic visualization produced the first spatiotemporal hologram (Kemp, 2008). Clearly, Harvard Laboratory, as a center for research and development, was a meeting place for GIS pioneers, spurring the development of computer software and geospatial analysis in the US (Kemp, 2008).

3.2.3. Experimental Cartography Unit (ECU)

Established in 1967, the Experimental Cartography Unit was a research entity in Britain's Natural Environment Research Council. It was established at the Clarendon Press with the goal of advancing "the art, science, technology, and practice of making maps by computers" (Kemp, 2008). David Bickmore founded the ECU after publishing *The Atlas of Britain*, a critical success but financial failure (Kemp, 2008). The experience led to his belief that computerized mapmaking was necessary, despite the fact that commercial software for such an undertaking was not yet available. He gained the support of the Royal Society, Britain's National Academy of Sciences, and the Natural Environment Research Council and succeeded in assembling a team of experts including "an optical physicist, a graphic designer, a computer scientist, and a software engineer, as well as assorted geographers and cartographers" (Kemp, 2008). Innovations and accomplishments associated with the ECU include: early studies in perception psychology; innovative map design and color schemes; the first digitizing production line; studies in automated contouring; the first automatically created multicolor map; and the development of databases and tools for data integration (Kemp, 2008).

3.2.4. US Bureau of the Census

Nearly concurrent with developments at CGIS, Harvard Laboratory, and ECU, major changes in data collection at the US Bureau of the Census were underway, including the introduction of GBF-DIME (Geographic Base File, Dual Independent Map Encoding) files in the late 1960s (GIS History Project, 2008). DIME files coded street segments between intersections, numbering the areas at either side of the segments and the nodes at either end of the segments. This technological innovation proved revolutionary in the field of GIS, corresponding to the arc structure of modern vector GIS, including DLG (USGS Digital Line Graphs), SDTS (Spatial Data Transfer Standard), and the polygons of ARC/INFO and other commercially available systems (GIS History Project, 2008).

DIME files led to the introduction of the TIGER (Topologically Integrated Geographic Encoding and Referencing) system in 1990 (GIS History Project, 2008). A comprehensive spatial database, Tiger files are the basis of the National Spatial Data Infrastructure (NSDI), which houses geographic coordinates and attributes of "transportation features...hydrographic features, address ranges, landmarks, and legal, statistical, and administrative entity boundaries" for the entire US and its territories (Kemp, 2008). The Census Bureau files are the foundation of the geo-demographics industry, which grew in large part from "the push to promote the use of Census data in the private sector" (GIS History Project, 2008). Documentation exists connecting the growth of the industry with census data workshops presented by the Bureau of the Census during the 1970s (GIS History Project, 2008). DIME and TIGER files are also considered influential in the commercial development and application of street network databases, mapping and routing services, and automobile navigation systems (University of British Columbia, Department of Geography, 2008).

3.2.5. Minnesota Land Management Information System

An interesting departure from early vector data based GIS, the Minnesota Land Management Information System (MLMIS), established in the 1960s, was raster based, using a grid of 40-acre cells corresponding to tax assessment districts. MLMIS, a project of the University of Minnesota's Center for Urban and Regional Affairs in conjunction with the Minnesota State Planning Agency, produced influential groundbreaking studies related to controversial land use problems, including timber industry issues and lakeshore development issues. MLMIS exists today as the Land Management Information Center-LMIC (GIS History Project, 2008).

3.2.6. Triangulated Irregular Networks

Representing another major development in GIS, Triangulated Irregular Networks (TINs) are vector-based representations of topographic elevations wherein irregularly distributed nodes and lines are arranged in non-overlapping triangles. TINs are generally derived from raster-based Digital Elevation Models, and the nodes and lines of which they consist have three-dimensional coordinates (x, y, and z) (Lecture, EES 4096G, 2008). Although TIN was developed independently by several different research groups, Thomas Poiker of Simon Fraser University, Canada, is most often credited with its invention. Surprisingly, Poiker's research was funded as a non-classified project by the Office of Naval Research, an agency of the US Defense Department, and although not identified as such, its focus is believed to have been a "slightly disguised version of the cruise missile guidance problem" (GIS History Project, 2008). Later incorporated into a commercial software package (ARC/INFO), one major innovation TIN offers is its ability to approximate terrain while requiring far less data storage capacity than that necessary for raster based DEMs (Kemp, 2008).

3.2.7. GIS Software

Decidedly the most significant software innovation was developed by Environmental Systems Research Institute, Inc. (ESRI). Founded in 1969 as a privately owned consulting firm by Jack and Laura Dangermond, ESRI was based on ideas developed at Harvard Laboratory and other research centers (University of British Columbia, Department of Geography, 2008). ESRI's original focus was on the organization and analysis of geographic information in both raster and vector formats, primarily in the area of landuse (Kemp, 2008). ARC/INFO, first released in the early 1980s, combined a relational database management system (INFO), for the handling of attribute tables, with software designed to handle objects stored as arcs (ARC). ESRI's phenomenal success was based in part on the fact that it offered the first GIS supported by personal computers (University of British Columbia, Department of Geography, 2008).

Earth Resources Data Analysis Systems (ERDAS), a division of Leica Geosystems of Switzerland, provides software for multispectral image analysis integrated with raster GIS. ESRI and ERDAS have worked closely since the early 1980s to develop interactive capabilities for the software they produce (Kemp, 2008).

Intergraph Corporation, originally founded in 1969 as M & S Computing, has been a leader in software designed for spatial information management and GIS. Early work included assisting the US Army and NASA in developing a digital real-time missile guidance system. Beginning with its first commercial contract in 1973 to map the City of Nashville, the company's focus switched to mapping applications, providing both software and hardware products. The company developed the first interactive CAD product in the 1980s and produced the first Pentium based workstations for the GIS industry in 1994 (Kemp, 2008).

More recently developed GIS software, IDRISI, is produced by Clark Labs, a non-profit research and development laboratory within the Graduate School of Geography at Clark University. Named for Abu Abdallah Muhammed al-Idrisi (1100-1166), Arab geographer and explorer, the software has evolved into an internationally used GIS with both geospatial data analysis and remote sensing capabilities (Kemp, 2008).

3.2.8. Geography's Quantitative Revolution and the Emergence of Critical Geography

The birth of modern GIS in the early 1960s coincides with the emergence of the Quantitative Revolution in Geography. Following the 1950s crisis, marked by the closing of Geography departments at universities around the country, including at Harvard, the quantitative revolution of the 1960s sought to make Geography less descriptive and more scientific, by emphasizing the importance of statistical analysis. Geographers emphasized the use of mathematical and statistical models, borrowing ideas from theories originating within the discipline of Economics.

Critical Geography, a major turning point in the history of the discipline, emerged in response to perceived overuse of statistical methods and mathematical models, particularly with regard to human geography. More specifically, in response to the rapid growth of GIS, the early 1990s witnessed the development of Critical GIS, a subfield concerned with addressing social and political implications of geographic information science. Concerns about ethics, social justice, and privacy, as well as issues regarding ontology and epistemology became the focus of Critical GIS, with Public Participation GIS one familiar result of the movement (Kemp, 2008).

3.2.9. US Department of Defense

Possibly the most significant driving force behind the development of modern GIS is US Department of Defense (DoD) sponsored research. DoD research is responsible for major advances first in aerial photography and then in space satellites for surveillance purposes. DoD sponsored research also resulted in the development of the Global Navigation Satellite System (GNSS), of which the Global Positioning System (GPS) is the first fully operational component (Kemp, 2008). Designed to aid in positioning, navigation, and timing, GPS is run by the DoD using a constellation of satellites allowing global coverage (GIS Development, 2008; Kemp, 2008). The information provided by aerial and satellite remote sensors, along with the ease of data collection based on GPS, has revolutionized GIS.

3.3. GIS and GISci Technology Present and Future

Through commonality of place, GIS and GISci allow routine combination and analysis of information from any number of databases, thereby providing an exceptional analytical tool for government, researchers, private industry, and individual citizens. With roots in computer mapping software, GIS has grown into a multi-billion dollar business with the probability of continued rapid growth (Bossler et. al., 2001). Empowered by advances in computing and the internet, it is a significant contributor to the US economy (Curry, 1997). Nourished by rapid increases in the variety and volume of geographic data, new applications, along with new ways of storing, processing, analyzing, modeling, visualizing, and transmitting geographic data, continue to emerge (Wilson and Fotheringham, 2008).

3.3.1. The "Data- and Computation-rich" GISci Environment

The environment within which GIS is currently practiced is one of unprecedented wealth in terms of data products and data sources, as well as in terms of computing power. Perhaps the greatest challenge associated with the ever-growing wealth of data and data sources is efficient and productive handling of the data. Secure and efficient management, including storage, organization, integration, and retrieval of large volumes of data pose significant challenges. The transformation of data into usable knowledge is a further challenge, often accomplished through Geographic Knowledge Discovery (GKD), defined as "the process of extracting information and knowledge from massive geo-referenced databases" (Miller, 2008). GKD includes Geographic Data Mining, the extraction of hidden patterns in data (Miller, 2008). Spatial Cluster Analysis, a rapidly evolving field within GISci, is also used for pattern recognition and data reduction (Jacquez, 2008). Other applications emphasize Dynamic Modeling, including Cellular Automata and Agent-based Modeling Systems, which are information technology-related approaches designed to merge spatial and temporal aspects of geographic data (Albrecht, 2008). Additionally, Object-oriented approaches attempt to capture change in spatial objects by "time-stamping" objects or their attributes (Albrecht, 2008). This "renaissance of 'time geography'" represents an attempt to incorporate the concepts of process and change in geographic spatial modeling (Albrecht, 2008).

3.3.2. Institutional GIS and GI Partnering

Institutional GIS is the term used to denote permanent technical and organizational structures which have evolved over time and which support Geographic Information (GI) practices, particularly in the public sector (Tulloch, 2008). Institutional GIS provides the necessary support for public resource decision making. Integral to institutional GIS is GI Partnering, which describes the relationships formed between and among institutions and individuals for data exchange and project collaboration, for example, between local and state governments (Tulloch, 2008).

Much of the research surrounding spatial data infrastructures (SDIs) has been driven by the needs of Institutional GIS (Tulloch, 2008). Defined as a "framework of technologies, policies, standards, and human resources necessary to acquire, process, store, distribute, and improve the use of geospatial data across multiple public and private organizations," SDIs represent the convergence of data, metadata, geospatial tools, and GIS practitioners (Wade and Sommer, 2006). The preference of the GIS community for timely and seamless access to locally produced data is believed attainable through National and Global Spatial Data Infrastructures. The general strategy is to have local communities retain control of coordinated and nationally standardized data and data processes and for this model to be extended globally (Tulloch, 2008). Despite the obvious difficulties in fully implementing this strategy, documentation exists of more than 50 countries maintaining "national spatial data clearinghouses" (Tulloch, 2008).

3.3.3. Public Participation GIS (PPGIS) and Participatory Decision-Making

As indicated above, one result of Critical GIS was the conceptualization of Public Participation GIS. PPGIS was a product of the GIS and Society Debate, an academic debate which emerged during the latter half of the 1980s (Weiner and Harris, 2008). The focus of PPGIS remains the linking of communities with GIS and other geospatial technologies for the purpose of empowering marginalized populations through geographic education. The intention is to engage the population using spatial and visual tools, including maps and satellite imagery, in order to promote community awareness and involvement on a local level, ultimately effecting social change (Weiner and Harris, 2008). As a means of participatory group decision-making, PPGIS continues to gain importance, with varied forms emerging around the world (Jankowski and Nyerges, 2008). PPGIS projects are recognized as “purposefully value-laden” exercises which “redefine the meaning of ‘accuracy’” (Weiner and Harris, 2008). Further controversy has arisen from concern that overemphasis on the perceived and real value of PPGIS could undermine healthy debate regarding the societal effects of some GIS practices (Weiner and Harris, 2008).

3.3.4. Web-based GIS, the Geospatial Semantic Web, and the Grid

Early geographic information systems were generally viewed as a resource used only by professionals. Essentially, a GIS was a closed system available within a particular organization. The internet and the worldwide web transformed GIS by opening these systems, changing the ways in which they are used, and increasing potential applications. In contrast to early geographic information systems, which were self-contained and project-based, web based GIS can be accessed by multiple users from multiple locations, accessing remotely located data sources and utilizing remotely located processing capabilities (Jones and Purves, 2008). Consequently, web based GIS facilitates access both within organizations and between organizations, as well as access by the public at large. The web for example, has become a resource for online mapping services, a means of querying and visualizing geographic information, and a source of spatial data including maps and digital images.

One major challenge in web-based GIS is to solve problems of compatibility and interoperability resulting from the need to integrate data from disparate sources and software (Jones and Purves, 2008). The concept of a Geospatial Semantic Web is based on the translation of data descriptions, or metadata, into a standardized formal language, thereby allowing all computers to understand and process the data (Fonseca, 2008). Ideally, the building of a Geospatial Semantic Web will result in easier access to data.

Such a construct would allow computers to function more like people, by implementing in computers "something similar to the human use of metaphors of space and time" (Fonseca, 2008).

A somewhat related concept is that of the Grid, "a term that encompasses a range of technologies and research efforts aimed at integrating the distributed computing resources of widely dispersed communities into transparent wholes" (Goodchild, 2008). It appears that feasibility of the Grid may rest on construction of the Semantic Web.

3.3.5. GIS and Location-based Services (LBS)

GIS clearly functions as an integrating platform for various data sources, technologies, and organizations. Location-based services (LBS), which can be defined as "technologies that add geographical functions to other technologies" have emerged from the integration of GIS, the internet, and new information and communications technologies (NICTs) including, but not limited to, location-aware mobile phones, personal digital assistants (PDAs), and navigation devices which also incorporate wireless information and communications technologies (Harvey, 2008; Brimicombe, 2008).

LBS applications currently available or under development include: navigation; wayfinding; real time tracking of vehicles, resources, and people; coordination of emergency and maintenance response; mobile commerce (in-transit business transactions and focused location-based marketing); location-based differential pricing of road use fees and car insurance premiums; and user solicited information for business or social purpose (Brimicombe, 2008).

3.3.6. Continuing Integration and the Application of Spatialization to Non-geo-referenced Phenomena

The direction of innovation in GIS appears to be towards continued integration of geographic information and concepts into other platforms. Particularly intriguing is the possibility of "cross-fertilization of research" through the use of GIS to formally integrate spatial concepts into study areas not traditionally conceived of as having geographic context (Goodchild, 2008). Traditional geographic concepts of location, distance, pattern, and scale are being applied to objects, phenomenon, and processes both tangible and abstract and both geo-referenced and non-geo-referenced (Skupin and Fabrikant, 2008). Examples include the Internet and cyberspace, the molecular structure of the human genome, human brain mapping, global communications flows, and real-time stock market transactions (Skupin and Fabrikant, 2008; Goodchild, 2008). Thus, future innovation is likely to include not just seamless integration of data, data sources, and technologies, but also the application of spatial metaphors for knowledge elicitation from massive and complex databases of inherently non-spatial data (Skupin and Fabrikant, 2008).

3.4. Endnotes

ALBRECHT, J., 2008, Dynamic Modeling, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 436, 438-439.

BOSSLER, J. D., JENSEN, J. R., MCMASTER, R. B., RIZOS, C., Eds., 2001, *Manual of Geospatial Science and Technology,* Taylor and Francis, New York, pp. 6, 401, 409.

BRIMICOMBE, A. J., 2008, Location-based Services and Geographic Information Systems, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 581, 583, 588-590, 592, 594.

CURRY, M. R., 1997, Digital People, Digital Places: Rethinking Privacy in a World of Geographic Information. *Ethics & Behavior*, 7: 253-264.

FONSECA, F., 2008, the Geospatial Semantic Web, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 367, 376.

GIS DEVELOPMENT, [http://www.gisdevelopment.net/history], accessed November 4, 2008.

GIS HISTORY PROJECT, University of Buffalo, [http://www.ncgia.buffalo.edu/hishist/barharbor.html], accessed November 4, 2008.

GOODCHILD, M. F., 2008, Geographic Information Science: The Grand Challenges, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 603-604.

HARVEY, F., 2008, *A Primer of GIS: Fundamental Geographic and Cartographic Concepts,* The Guilford Press, New York, pp. 145-148, 292.

JACQUEZ, G. M., 2008, Spatial Cluster Analysis, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 413.

JANKOWSKI, P., NYERGES, T. L., 2008, Geographic Information Systems and Participatory Decision Making, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 491.

JONES, C. B., PURVES, R. S., 2008, Web-based Geographic Information Systems, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 559, 578.

KEMP, K., Ed., 2008, *Encyclopedia of Geographic Information Science,* Sage Publications, Los Angeles, pp. 18-19, 56-57, 126-128, 135-136, 188, 215, 219-220, 223-224, 233, 477, 491.

KORTE, G. B., 2001, *The GIS Book, 5th Ed.,* Onword Press, Albany, NY, p. 401.

LECTURE, University of New Orleans, EES 4096G, November 11, 2008.

MILLER, H. J., 2008, Geographic Data Mining and Knowledge Discovery, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 352, 358.

SKUPIN, A., FABRIKANT, S., I., Spatialization, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 61, 77.

TULLOCH, D. L., 2008, Institutional Geographic Information Systems and Geographic Information Partnering, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 449, 457-458.

UNIVERSITY OF BRITISH COLUMBIA, DEPARTMENT OF GEOGRAPHY, History of GIS, [http://www.geog.ubc.ca/courses/klink/gis.notes/ncgia/u23.html#SEC23.1], accessed 11/4/08.

WADE, T., SOMMER, S., Eds., 2006, *A to Z GIS*. ESRI Press, Redlands, CA, p. 187.

WEINER, D., HARRIS, T. M., 2008, Participatory Geographic Information Systems, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 466, 475-476.

WILSON, J. P., FOTHERINGHAM, A. S., Eds., 2008, *The Handbook of Geographic Information Science*, Blackwell Publishing, Malden, MA, pp. 1, 7, 352.

Chapter 4

The Global Positioning System

4.1. The Global Positioning System Defined

The Global Positioning System (GPS), the only fully operational Global Navigation Satellite System, is officially named NAVSTAR GPS. Described as "a space based positioning, navigation and timing system," it is a constellation of 24 satellites in precisely known orbits (GIS Development, 2008; Kemp, 2008). Originally developed for defense purposes to accurately locate military assets, the first GPS satellite was launched in 1978 (Brimicombe, 2008; Monmonier, 2002). Today GPS is maintained by the Department of Defense, with an annual budget of approximately $400 million, and is freely available throughout the world (Harvey, 2008). Estimated to have cost over $10 billion to develop and implement, the GPS system originally offered two-tiered service, with military applications accessing the Precise Positioning Service (PPS), while civilian applications made use of the Standard Positioning Service (SPS), a more easily jammed and less accurate data version (Monmonier, 2002). This Selective Availability proved both costly and unnecessary, with the shortage of PPS receivers during the 1991 Gulf War requiring reduction of signal degradation to SPS receivers, and with the ability of SPS receivers, in any case, to obtain near military accuracy by linking to precisely located ground stations (Monmonier, 2002). While Selective Availability was switched off in May, 2000, the US military maintains control of the system, with ready capability to implement regional or global Selective Availability during national security crises (Monmonier, 2002).

GPS applications include navigation, mapping, surveying, in-situ data collection, and other precise positioning applications. The process by which GPS is used to determine location is referred to as "satellite ranging" (Lillesand et.al., 2008). It involves the transmission of time encoded radio signals from the satellites to ground-based receivers the size of a postage stamp with an antenna, and the use of triangulation (Lillesand et. al., 2008; Harvey, 2008). Because satellite location is precisely known, using the speed of radio signal travel (the speed of light), along with the comparison of satellite and receiver time data, distance from the satellite to the receiver can be calculated (Lillesand et. al., 2008). A signal reading from one satellite allows for the computation of a sphere with the satellite at its center and a radius equal to the distance from satellite to receiver. The receiver's location is somewhere on that sphere (Harvey, 2008). Since the orbits of the constellation satellites insure that five to eight satellites are always visible from any point on the earth's surface, signals from additional satellites are readily available for the calculation of additional spheres (Brimicombe, 2008). Intersections of three calculated spheres, from three satellite signals, determine two possible locations of the receiver. Given general knowledge of the receiver's location, one of those possibilities can usually be eliminated. As a result, location can generally be determined using triangulation and GPS signals from three satellites. The use of four GPS satellite signals is preferable, allowing location determination without knowledge of the receiver's general location, while also correcting for any lack of synchronicity between satellite atomic clocks and lower accuracy GPS receiver clocks (Lillesand et. al., 2008). Furthermore, this three-dimensional triangulation allows for elevation estimation, in addition to estimation of latitude and longitude (Monmonier, 2002). And, in instances where elevation is known, only two satellites are necessary to determine receiver location (Harvey, 2008).

The positional accuracy of GPS is influenced by several factors, including atmospheric interference, multipath error introduced when signals are reflected from the ground or other surfaces prior to reaching the receiver and obstruction of signals by buildings, tree cover, and other elements in the environment. Additionally, the quality of the GPS receiver, movement of the GPS receiver, "satellite ephemeris errors" which are "uncertainties in the satellite orbits", and clock bias all affect GPS accuracy (Lillesand et. al., 2008). Positional Dilution of Precision (PDOP) is a measurement used to represent the sum of those errors, with PDOP values less than 4 indicating a high degree of accuracy and values greater than 8 indicating a low degree of accuracy in GPS readings (Harvey, 2008).

Mitigating for error in GPS readings involves the calculation of differential GPS measurements based on simultaneous measurements taken by one or more portable GPS receivers and by a stationary base receiver at a precisely known location. Corrections to the portable GPS receivers' readings are made based on positional errors detected for the stationary base receiver. While corrections may be made post-processing, real-time differential GPS positioning involves the instantaneous broadcast of base station corrections to portable GPS receivers (Lillesand et. al., 2008).

The Wide Area Augmentation System (WAAS), consisting of approximately 25 base stations and available throughout North America, is the most common differential GPS system, allowing for accuracy, in some cases, down to centimeters or inches (Lillesand et. al., 2008; Harvey, 2008). Within the WAAS system, master stations on the east and west coasts collect data from the network stations, then calculate and broadcast location specific correction signals for use by WAAS enabled GPS receivers (Lillesand et. al., 2008). While strong WAAS signals increase accuracy, because the correction signals are broadcast via geostationary satellites located over the equator, obstructions on the horizon can weaken the signal and, in some instances, cause more error with the WAAS correction than without it (Lillesand et. al., 2008). Still, PDOP values less than 4 may yield locational accuracy down to 1 or 2 meters (Harvey, 2008).

The National Geodetic Survey's Continuously Operating Reference Stations (CORS) network is another accuracy augmentation system consisting of 800 GPS base stations located throughout the US. CORS provides differential correction data via the internet for use in postprocessing (Lillesand et. al., 2008).

4.2. The Future of GPS

Efforts to overcome the shortcomings of GPS are likely to trend towards the integration of existing and future technologies. The major drawback of GPS is the necessity of a clear view of the sky. Because GPS receivers will not function indoors and function only poorly in forested areas, “urban canyons” and other obstacle laden landscapes, research is currently underway to integrate GPS with the telecommunications network (Brimicombe, 2008). In the US, the nation-wide cellular base station network is made up of cells, each of which has a unique ID called a cell global identity (CGI). A mobile phone is automatically registered to the cell within which it is located, with that registration changing as the phone moves from one cell to another. While urban cells may have a radius of 100 meters, rural areas may have cells as extensive as 30 kilometers. More precise estimation of mobile phone location is possible, however, when cell ID is augmented by the phone’s timing advance and the direction from which the signal is received. Timing advance is a means of regulating the timing of signal transmission to insure that phones using a particular cell at the same time and operating at the same wavelength will not interfere with each other. Because a mobile phone maintains contact with several base stations to insure smooth transition between cells, timing advance can be used to estimate the distance of the phone from network base stations. By triangulating the estimates for three base stations, the phone’s location can be estimated within about 20 meters (Brimicombe, 2008). While both GPS and network based approaches have disadvantages, it is theorized that present methods of coupling the two may yield locational accuracy of 10 to 15 meters (Brimicombe, 2008).

4.3. The Future of Global Navigation Satellite Systems

Currently, the only counterpart to the US GPS is Russia’s GLONASS system, a constellation of 24 satellites, of which 13 are operational. A cooperative effort between Russia and India is underway to launch additional satellites to make the system fully operational (Lillesand et. al., 2008). Other GNSSs under development include Galileo, the European system consisting of 30 satellites scheduled for full operation by 2010, the Compass/BeiDou Navigation Satellite System (CNSS), an expansion of the Chinese regional system scheduled for global operation within the decade, and the Indian Regional Navigation Satellite System (IRNSS), scheduled for full operation by 2011 (Lillesand et. al., 2008; Hegarty and Chatre, 2008). Additionally, the Quasi-Zenith Satellite System (QZSS) under development in Japan will provide limited geographic coverage and be fully operational within the next decade (Hegarty and Chatre, 2008).

Counterparts to the US WAAS system include Japan's Multifunctional Satellite Augmentation System (MSAS) and the European Geostationary Navigation Overlay Service (EGNOS), both of which use geostationary satellites for broadcast of real-time differential correction signals (Lillesand et. al., 2008). India's GEO Augmented Navigation (GAGAN) system is currently under development and expected to be operational by 2010 (Hegarty and Chatre, 2008).

Trends towards compatibility, integration, and interoperability will likely not be limited to GPS applications within the US. Instead, emerging Global Navigation Satellite Systems are being designed for global compatibility and interoperability. If attainable, interoperability would allow systems to be used either separately or in conjunction, without interference or degradation of performance. Integration and interoperability would likely be synergistic, resulting in greater capabilities and service to the users.

4.4. Endnotes

BRIMICOMBE, A. J., 2008, Location-based Services and Geographic Information Systems, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 581, 583, 588-590, 592, 594.

GIS DEVELOPMENT, [http://www.gisdevelopment.net/history], accessed November 4, 2008.

HARVEY, F., 2008, *A Primer of GIS: Fundamental Geographic and Cartographic Concepts,* The Guilford Press, New York, pp. 145-148, 292.

HEGARTY, C. J., CHATRE, E., 2008, Evolution of the global Navigation Satellite System (GNSS). *Proceedings of the IEEE* 96: 1902-1917.

KEMP, K., Ed., 2008, *Encyclopedia of Geographic Information Science,* Sage Publications, Los Angeles, pp. 18-19, 56-57, 126-128, 135-136, 188, 215, 219-220, 223-224, 233, 477, 491.

LILLESAND, T. M., KIEFER, R. W., CHIPMAN, J. W., 2008, *Remote Sensing and Image Interpretation*, *6th Edition*, John Wiley & Sons, Hoboken, NJ, pp. 42-45, 59-61, 401-403, 471.

MONMONIER, M., 2002, *Spying with maps.* The University of Chicago Press, Chicago, pp. 12-15, 18-19, 22-30.

Chapter 5

Privacy

5.1. Privacy Defined

The concept of privacy has been called "exasperatingly vague and evanescent" and "infected with pernicious ambiguities" (Solove, 2008). It has been broadly defined as "the right to be let alone" and narrowly defined as covering "intimate information, access, and decisions" (Solove, 2008). Considered culturally universal, the desire for privacy nevertheless finds its expression in culturally specific mechanisms (Altman, 1977). And, while the tension between seclusion and interaction is found in all human society, it is evident also among animals (Lanier and Saini, 2008). Still, despite the attention it has received, dating at least to Aristotle, who distinguished the family from the public and the private from the political, the concept of privacy remains a conundrum for contemporary society (O'Brien, 2008).

Many definitions of privacy have as their emphasis, the individual, characterizing privacy as a "sanctuary" or "safe haven" from scrutiny (Nissenbaum, 1998). Others view privacy as more than just the right of individuals, considering it "a form of freedom built into the social structure" (Karyda et. al, 2007). Some scholars bypass laborious attempts to conceptualize privacy, proceeding to the analysis of commonly recognized privacy issues (Solove, 2008). Others, despairing of ever defining the essence of privacy, advocate a pluralistic conceptualization. Solove (2008), characterizing the search for a definition as a "rather fruitless and unresolved debate," determines that "The term privacy is best used as a shorthand umbrella term for a related web of things. Beyond this kind of use, the term privacy has little purpose. In fact, it can obfuscate more than clarify" (Solove, 2008). Still, arguments for a unitary concept persist, with some calling for broad conceptualization based on protection of human dignity and control over autonomy and accessibility (Lanier and Saini, 2008). Thus, the search continues, based in part on the conviction that a clear conceptualization of privacy is a fundamental prerequisite for solving privacy issues.

In his theory of privacy, social psychologist Irwin Altman (1977) calls privacy "a dialectic interaction with others," and a "boundary control process." He defines privacy as "the selective control of access to the self." According to Margulis (2003), legal scholar Alan Westin likewise considers privacy a dynamic process, and defines it as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." While Altman and Westin have both contributed to contemporary conceptualizations of privacy, Westin's theories have been particularly influential with regard to the balancing of privacy and technology. This is evident in a survey of contemporary, somewhat less formal definitions of privacy, which include, "the individual's ability to control the terms by which their personal information is collected and used," and the ability to protect ourselves from "being simplified and objectified and judged out of context" (Karyda et al., 2007; Rosen, 2000). Most notably, Fenwick considers "informational autonomy," i.e., the right to control information about ourselves, to be the "central privacy issue" (O'Brien, 2008). For Karyda, et. al. (2007) who recognize four types of privacy (bodily, territorial, communication, and informational privacy), control over information remains a defining characteristic of privacy.

5.2. The Value of Privacy

Certainly less controversial than its conceptualization, is the recognition of privacy's value at the individual and societal levels. While common conceptions of privacy frequently focus on secrecy and individuals, the functions of privacy are more complex.

Altman's (1977) privacy theory describes three functions of privacy: "(a) management of social interaction, (b) establishment of plans and strategies for interacting with others, and (c) development and maintenance of self-identity." Westin's more detailed theory, as described by Margulis (2003), defines four states of privacy through which the functions of privacy are achieved. They include:

solitude (freedom from observation); *intimacy* (seclusion within a small group); *anonymity* (freedom from identification and surveillance in public); and *reserve* (the desire to limit self-disclosure). According to Margulis (2003), Westin outlines the functions of privacy as follows: *personal autonomy*, which allows individuals to avoid domination, manipulation, or exposure; *emotional release* from the tensions of social life, which allows the management of losses, as well as of bodily functions; *self-evaluation*, which allows individuals to process information, integrate experiences, and engage in moral and religious contemplation; and *limited and protected communication*, which allows the setting of personal boundaries and the safe exchange of sensitive information.

Aspects of both Altman's and Westin's theories are evident in many references to the value of privacy. Generally considered essential to the development and survival of healthy individuals and critical to the proper functioning of society, privacy promotes not just autonomy, individuality, creativity, and productivity, but civility as well, by establishing boundaries of conduct for social interaction. Privacy also promotes just government.

On the personal level, privacy makes respect, trust, friendship, and love possible by allowing controlled, gradual disclosure of oneself to another (Rosen, 2000). In addition to fostering and protecting intimate social relationships, privacy also protects other important social relationships including business and professional relationships (Rosen, 2000). It additionally protects the individual from overwhelming pressures towards social conformity as well as from misjudgments based on too much, too little, or incorrect information (Rosen, 2000). Therefore, in addition to fostering individuality, autonomy, and creativity, privacy promotes mental health, healthy social relationships, peaceful interactions, and happiness as well.

On the societal level, privacy fosters the freedom essential to a fully functioning democratic society by allowing individuals to control information about themselves and their affiliations. Such control prevents objectification of the individual and promotes the balance of power between individual and government (Rosen, 2000). Nissenbaum notes that “privacy is an important means by which individuals may sustain power, liberty, and autonomy against potentially overwhelming forces of government” (Nissenbaum, 1998). Rosen further states that:

> By insisting that there are personal boundaries that the state may not overstep, interior regions into which it cannot penetrate, liberalism expresses its respect for the inherent dignity, equality, individuality, interiority, and subjectivity of the individuals who compose it. Inviolability is a form of equality; people who are less than equal are people who can be violated.” (Rosen, 2000)

It is on this basis that privacy is considered a fundamental human right, universally recognized in major treaties and human rights agreements (Karyda et. al., 2007). While these conceptualizations of privacy tend to characterize the relationship between the individual and society as antagonistic, Solove offers another viewpoint, clearly articulating the value of privacy to both the individual and to society by stating that:

> Privacy is not simply a way to extricate individuals from social control, as it is a form of social control that emerges from a society’s norms. It is not an external restraint on society, but is in fact an internal dimension of society. Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society…. Privacy issues involve balancing societal interests on both sides of the scale. (Solove, 2008)

In other words, privacy provides a means of social control through which protection of the individual also constitutes protection of the society. The challenge, therefore, is to balance society’s interest in protecting the individual with society’s interest in protecting society at large. Perhaps the most prominent example of this challenge is society’s struggle to balance privacy and security.

5.3. The Legal Basis of Privacy in the United States

While most Americans assume their right to privacy, neither the Declaration of Independence nor the Constitution of the United States guarantees such a right. In fact, the word *privacy* does not appear in either document (Holtzman, 2006). Instead, in the United States the common law protection of privacy is based upon civil law torts, while protection afforded by federal laws proceeds from interpretations of the Bill of Rights, the Amendments to the Constitution (Holtzman, 2006).

5.3.1. Privacy and Civil Law: The Four Torts

The origins of judicial privacy are based on the landmark 1890 *Harvard Law Review* article by law partners Samuel Warren and Louis Brandeis, future US Supreme Court Justice. Their article, "The Right to Privacy" was a response to what they perceived as threats to privacy due to "numerous mechanical devices," including cameras allowing "instantaneous photographs" (Warren and Brandeis, 1890; Holtzman, 2006; Lanier and Saini, 2008). Warren and Brandeis defined privacy as "the right to be let alone" and viewed privacy violations as the unwelcome exposure of information (Warren and Brandeis, 1890; Holtzman, 2006). They promoted the concept of the "inviolate personality," respect for which required acknowledgement of a "protected field of decision making" necessary for the conduct of life and the achievement of happiness (Warren and Brandeis, 1890, O'Brien, 2008). While recognizing individual responsibility for privacy, their article called for government intervention when individual control of privacy is rendered ineffective, for instance, by technological advances (Holtzman, 2006). Their article provided the foundation for US tort law by laying the groundwork for private lawsuits (Holtzman, 2006).

A tort can be thought of as a wrongful act which is not a breach of contract, but is instead a private or civil injury (Merriam-Webster Online, 2009; Holtzman, 2006). According to Holtzman (2006), a significant advancement in privacy law occurred in 1960 when legal academic Dean William Prosser proposed that a privacy tort actually combines four distinct torts: appropriation; intrusion; disclosure; and false light. Appropriation is the use of a person's identity or likeness for commercial purposes without authorization (Holtzman, 2006; Lanier and Saini, 2008). Intrusion is the literal or figurative invasion of an individual's solitude, seclusion, or private space (Holtzman, 2006; Lanier and Saini, 2008). Disclosure involves the public release of private facts or information of an intimate nature which is not of legitimate concern to the public (Holtzman, 2006; Lanier and Saini, 2008). And false light is the public portrayal of a person inaccurately and negatively. False light falls just short of defamation, which additionally requires damage to reputation (Holtzman, 2006; Lanier and Saini, 2008). According to Lanier and Saini (2008), Prosser's framework effectively restricts privacy tort violations to individual-level data which is deemed private but has been publicly disseminated. By excluding data freely disclosed, as well as aggregated data, in most cases this narrow framework exempts collection and dissemination of consumer information (Lanier and Saini, 2008).

5.3.2. Privacy and the Constitution

Throughout US history, judicial interpretation of the Bill of Rights has afforded some privacy protection. Privacy protections rooted in the Bill of Rights include the First Amendment's implicit protection of the right of association, the Fourth Amendment's protection against unreasonable searches and seizures by the government, the Fifth Amendment's protection against self-incrimination, the Fourteenth Amendment's due process clause effectively obligating states to comply with federal restrictions imposed by the Bill of Rights, and the Ninth Amendment, addressing rights not specifically enumerated in the Constitution (Holtzman, 2006).

5.3.3. Privacy and Federal Legislation

Federal legislation has significantly impacted privacy, beginning most notably with the Freedom of Information Act (FOIA), passed in 1966 allowing universal access to the records of federal agencies, including birth, death, marriage, drivers, real estate transactions, and tax records, among others, and the Privacy Act of 1974, an amendment to the FOIA, created primarily to prevent unauthorized release of personal information by government agencies (Nissenbaum, 1998; Holtzman, 2006; Lanier and Saini, 2008). The Privacy Act was heavily influenced by the Fair Information Practices (FIPs) formulated in 1973 as a result of investigation by the Department of Health, Education, and Welfare into the need for safeguards against potentially harmful consequences of newly automated public and private data collection (Lanier and Saini, 2008). According to Smith (2004), the FIPs covered several areas of data management, including: collection limitation (a ban of secret record keeping); disclosure (the ability of individuals to access their records); secondary use (the means of preventing the use of information for purposes other than that for which it was originally collected); record correction (the ability of individuals to correct inaccurate information); and security (the assurance of secure creation, maintenance, use, and dissemination of personal data). As a result, the Privacy Act requires that notice be provided upon data collection, that only necessary and relevant data are collected, and that citizens and legal permanent residents are allowed to examine, and correct if necessary, any personal data collected by the government (Holtzman, 2006). The Privacy Act does, however, include major exceptions relative to national security, law enforcement, and the use of data from private corporations. Furthermore, it is important to note that only information stored in federal databases is subject to the Privacy Act (Holtzman, 2006). Commercial companies are subject neither to the Privacy Act, nor its subsequent amendment, the Computer Matching and Privacy Protection Act of 1988, which established procedural guidelines in the matching of electronic records (Holtzman, 2006). Both laws are circumvented by the US government through data partnerships between government agencies, including the FBI, the CIA, and the IRS, and private data-aggregation firms, allowing government access to enormous databases of personal information collected, maintained, and exchanged outside the protections of the Privacy Act. Because the government does not create or maintain the files, and instead merely contracts for access to the files, adherence to the provisions of the Privacy Act is not required by the government under these circumstances, just as it is not required by private industry (Holtzman, 2006).

Most privacy legislation, including the Privacy Act of 1974 which followed publicized FBI domestic-spying incidents including Watergate, has been passed in response to public outcry following highly publicized media events (Holtzman, 2006; Nissenbaum, 1998). One example is the Video Privacy

Protection Act of 1988, frequently referred to as the Bork Bill, due to its origins in response to the revelation of Associate Supreme Court Justice Nominee Robert Bork's video rental records (Nissenbaum, 1998). Another example is the Driver's Protection Privacy Act of 1994, passed in response to the murder of actress Rebecca Schaefer by a stalker whose hired private investigator had furnished him information freely available through the California Department of Motor Vehicles (Holtzman, 2006). The Children's Online Privacy Protection Act of 1998 is also an instance of reactionary legislation. Unfortunately, these "extremely narrow" laws, in addition to being riddled with exceptions (including, ironically, an exception for private investigators in the Driver's Protection Privacy Act), reflect a lack of public deliberation regarding privacy issues (Holtzman, 2006; Nissenbaum, 1998). Nissenbaum calls the result, "a body of policy that is piecemeal and inconsistent." However, despite recognition of the inadequacy of the existing patchwork of legislation, Rosen (2000) suggests that:

> Efforts to pass comprehensive legal protections for privacy haven't fared very well in America for a simple reason: although polls about privacy show that a majority of people claim to support it, many of the best-organized interest groups strenuously oppose. Corporations dislike privacy protections that would restrict their ability to use personal information in marketing schemes. Lobbyists for federal law enforcement are also powerful foes of privacy reform. (Rosen, 2000)

Such efforts are further complicated by the struggle to balance individual needs and the needs of the society at large, particularly, as previously mentioned, the struggle to balance privacy and security.

5.3.4. The USA Patriot Act

The official name of the Patriot Act is the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*. Introduced within a week of the attacks of 9/11 and signed into law shortly thereafter, the stated purpose of the Patriot Act is "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes" (Brown, 2003; Public Law 107-56).

The Patriot Act enhances the authority of federal law enforcement and intelligence-gathering agencies to search e-mail communications, telephone, medical, financial, library, and other records without court order (Keenan, 2005). It also expands the government's authority to obtain court orders for what has been termed "sneak and peak" searches, wherein homes are secretly searched with the possibility of property removal, with extensively delayed notification of the owners (Keenan, 2005). In addition, the Patriot Act sanctions the expanded use of National Security Letters (NSLs), administrative subpoenas which do not require probable cause or judicial oversight (Keenan, 2005; ACLU, 2009). Although NSLs originally contained clauses forbidding recipients to disclose the existence of the letters, that provision was ruled unconstitutional as a result of a lawsuit initiated by the American Civil Liberties Union (ACLU, 2009). And, because the Patriot Act also expands the definition of terrorism to include a vague description of domestic terrorism, the enhanced law enforcement powers allow unprecedented surveillance of American citizens, along with non-citizens (Keenan, 2005; ACLU, 2009).

Other controversial provisions of the Patriot Act include the authorization to collect and analyze DNA from all people convicted of violent crimes, and the expansion of law enforcement authority in the handling of immigrants and border control, allowing indefinite detention and/or deportation of immigrants under suspicion of aiding terrorism (Freedman, 2008).

Some provisions of the Patriot Act were given sunsets, meaning reauthorization is required after a specified period of time. The Patriot Act was reauthorized in 2006 and will again be up for reauthorization in 2009 (Keenan, 2005; ACLU, 2009).

5.3.5. Privacy Policies

Privacy policies are legal documents establishing how a customer's data will be handled by a vendor or website. They generally disclose what information is collected, how the information can be used, to whom the information can be disclosed, and how the information will be safeguarded. Unfortunately, privacy policies afford minimal protection to customers and maximum flexibility for vendors. According to Holtzman (2006), “they are effectively useless as protection against misuse of customer data by the company.”

5.3.6. Privacy Discrepancies between the US and the European Union

Privacy protection in the European Union contrasts sharply with US privacy policies. Unlike the US, which provides little to no protection for data privacy in the private sector, the EU, as early as 1995, formally recognized the importance of data privacy in the adoption of EU Directive 95/46/EC created for “the protection of individuals with regard to the processing of personal data” (Cannataci and Mifsud-Bonnici, 2005).   In the year 2000 the “right to the protection of personal data,” originally outlined in the European Union Charter of Human Rights, was incorporated into the Constitutional Treaty for Europe, making it a fundamental right and freedom protected at the constitutional level (Cannataci and Mifsud-Bonnici, 2005).

The discrepancy in the levels of data privacy protection in the US and the EU necessitated protracted negotiations lasting more than two years prior to the adoption of the Safe Harbor Principles in 2000 (McKenna, 2001).   Designed to demonstrate US business compliance with the 1995 EU data directive, the Safe Harbor Principles are similar in content to the Fair Information Practices discussed above, with the notable exception of the necessity of an effective means of enforcement, a provision lacking in the self-regulatory FIPs which are essentially recommendations unenforceable by law. In Europe the Safe Harbor Principles were “widely condemned as inadequate” (McKenna, 2001). Not surprisingly, by the end of the first year following adoption, only 48 US companies had registered as adherents to the Safe Harbor Principles (McKenna, 2001). Currently the US Department of Commerce website lists 262 firms on the Safe Harbor list, 218 of which are listed as having current certification. Although the website is designed to provide compliance data on each of the firms, apparently that information is currently unavailable (US Department of Commerce, 2009).

5.4. Endnotes

ACLU, [http://www.aclu.org], accessed June 21, 2009.

ALTMAN, I., 1977, Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues,* 33: 66-84.

BROWN, C., Ed., 2003, *Lost Liberties: Ashcroft and the Assault on Personal Freedom*. The New Press, New York, pp. 58.

CANNATACI, J., MIFSUD-BONNICI, J. P., 2005, Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty. *Information and Communications Technology Law*, 14: 5-15.

FREEDMAN, J. 2008. *America Debates Privacy versus Security*. New York: Rosen Central, p. 17.

HOLTZMAN, D. H., 2006, *Privacy Lost: How Technology is Endangering Your Privacy.* Jossey-Bass, San Francisco, pp. 8, 31, 93-117, 176-178.

KARYDA, M., GRITZALIS, S., PARK, J. H., 2007, A Critical Approach to Privacy Research in Ubiquitous Environments – Issues and Underlying Assumptions. *EUC Workshops 2007*, LNCS 4809, pp. 12-21.

KEENAN, K., 2005, *Invasion of Privacy.* ABC-CLIO, Inc., Santa Barbara, pp. 92-93, 210.

LANIER, C. D., SAINI, A., 2008, Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 12: 1-6.

MARGULIS, S. T., 2003, On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, 59: 411-429.

MCKENNA, A., 2001, Playing Fair with Consumer Privacy in the Global On-line Environment. *Information and Communications Technology Law*, 10: 339-354.

MERRIAM-WEBSTER DICTIONARY, [http://www.merriam-webster.com/], accessed June 21, 2009.

NISSENBAUM, H., 1998, Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17: 559-596.

O'BRIEN, M., 2008, Law, privacy and information technology: a sleepwalk through the surveillance society? *Information and Communications Technology Law,* 17: 25-35.

PUBLIC LAW 107-56, [http://www.gpo.gov/fdsys/pkg/LPAW-107publ56.pdf], accessed June 21, 2009.

ROSEN, J., 2000, *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, New York, pp. 8, 10, 12, 20, 216-217, 219, 169-170.

SMITH, J., MACKANESS, W., KEALY, A., WILLIAMSON, I., 2004, Spatial Data Infrastructure Requirements for Mobile Location Based Journey Planning. *Transactions in GIS,* 8: 23-44.

SOLOVE, D. J., 2007, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review,* 44: 745-772.

US DEPARTMENT OF COMMERCE, SAFE HARBOR LIST, [http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe=harbor=list?OpenDocument&Start=1], accessed June 18, 2009.

WARREN, S. D., BRANDEIS, L. D., 1890, The Right to Privacy. Harvard Law Review, 4: 1-23.

Chapter 6

The Impact of Geospatial and Ancillary Technologies on Privacy

6.1. Remote Sensing and Surveillance

6.1.1. Camera Surveillance

Broadly defined, remote sensing has wide application in contemporary society. An obvious example is camera surveillance, rapidly becoming a ubiquitous, yet generally overlooked feature of the landscape for the majority of Americans, with digital capabilities allowing nearly instantaneous delivery of visual images on site or to remote locations. We are photographed frequently in many locations, including banks and ATMs, retail outlets, corporate offices, hotel lobbies, government buildings, museums, on streets where we drive or walk, in elder care facilities, children's day care facilities, and even in some classrooms (Amato, 2001). Surveillance of prisoners is standard and surveillance of employees is not unusual. Many cameras are visible in these places, while others are hidden, such as the nearly 400 rotating cameras hidden in globes resembling street lights in New York City (Dority, 2001). The rapid increase in remotely sensed visual surveillance throughout the US is evident in the placement of cameras in housing projects in Boston and city buses in Portland, Oregon, and probably in every major urban center in between (Dority, 2001).

One reason frequently cited for camera surveillance is crime deterrence. The United Kingdom's first surveillance cameras were positioned in 1986 for just such a purpose. Considered successful, video surveillance in the UK has since become so pervasive that the country has more closed-circuit cameras per capita than any other country (Amato, 2001). It is estimated that Britons are photographed by 300 separate cameras each day (Armstrong and Ruggles, 2005).

A prominent example of mass surveillance and biometrics is the 2001 Super Bowl in which Tampa authorities imaged the faces of 100,000 attendees as they entered the arena, extracted eigenfaces, and compared the fan database to a database of known criminals. Obtained without the knowledge or consent of the fans, the exercise produced 19 possible matches, although no arrests resulted (Amato, 2001). Alarmed privacy activists, including the American Civil Liberties Union (ACLU), responded by calling attention to the lack of government regulation protecting citizens from misuse of this and related technologies (Dority, 2001). The ACLU also asserted that the attendees' Fourth Amendment rights "to be free of unreasonable searches and seizures" were violated and that the exercise could effectively be characterized as "a computerized police lineup as a condition of admission" (Dority, 2001). Also of fundamental concern was the disposition of the data collected.

6.1.2. DARPA, Biometrics, and Remote Recognition

Face-recognition technologies, which rely on breaking down, analyzing, and extracting patterns in digital images, are just one application of biometrics, defined as "automatic personal recognition based on physiological or behavioral characteristics" (Probhakar, et. al., 2003). In addition to face recognition, biometric pattern recognition can be applied to the voice, to the iris, and to body geometry, as well as to human behavior.

In 1997, the federal government, through the US Defense Advanced Research Projects Agency (DARPA) began funding a program to explore the feasibility of identifying a person from up to 150 meters away. An extension of the program, DARPA's *Human ID at a Distance,* has funded research at several universities within and outside the US for that purpose (Amato, 2001; Nixon and Carter, 2004). As part of the program, researchers at the University of Southhampton, UK have extensively studied human gait recognition as a means of identifying individuals based on the observation that while a face may be masked, disguising how a person walks or runs would be much more difficult (Nixon and Carter, 2004; Dority, 2001). Other research has included the use of "a video-based network of sensors" to measure individual body dimensions and to provide a kind of "body fingerprint" to facilitate recognition of individuals (Amato, 2001). DARPA has also funded research at the Georgia Institute of Technology for the development of “smart floors” with built in sensors to recognize people based on their “force profiles” (Amato, 2001). And the ambitious but likely attainable goal of DARPA funded Princeton researchers is to use a highly specialized camera to detect “patterns of color, striation and speckles in their irises” as a means of recognizing individuals from 100 meters away (Amato, 2001).

Perhaps the most alarming DARPA funded research relative to traditionally defined remote sensing is that conducted at Pittsburgh’s Carnegie Mellon University. As of 2001, researchers there were working to perfect a remote sensing system with hyperspectral scanning capabilities to measure reflectance from a person’s skin as a means of identification. Apparently, absorption and reflectance from an individual’s skin can provide a unique signature. At present, this signature can be read if a person sits still in a chair as the sensor sweeps over him for a period of about 5 seconds. The goal of this group of researchers is to find specific wavelengths which will allow the time required for identification to be reduced to a fraction of a second (Amato, 2001).

The integration of several different biometric capabilities results in what is termed “multi-modal biometric systems” which add greater accuracy in recognizing individuals (Probhakar, et. al., 2003).

6.1.3. Beyond Recognition to Discernment of Intention

Also alarming is research which seeks to recognize human emotion by way of facial expressions, ultimately leading to recognition of intentions (Amato, 2001). According to Jeffrey Cohn, a psychologist at Carnegie Mellon, his research is aimed at “developing computer systems that can detect human activity, recognize the people involved, understand their behavior, and respond appropriately” (Amato, 2001). Already, IBM markets to retail stores software that records shoppers’ eye movements and facial expressions as a means of discerning their preferences and predicting their buying habits (Amato, 2001).

6.1.4. Privacy Concerns Associated with Biometrics

Although recognition technologies based on remote sensing offer security and convenience in a number of commercial, governmental, medical, and forensic applications, critics point to several areas of potential abuse. A major concern associated with biometrics is that, because identifiers are primarily biological in origin, personal information from scanned biometric measurements may be extracted, and/or integrated with other data, and then used in a different context, for example, to draw inferences regarding health status or other personal characteristics. Such applications are assumed to tip the balance of power away from the individual in favor of governmental or corporate entities. Also, most would consider it an invasion of privacy if a person's ability to remain anonymous is denied by biometric recognition (Prabhakar et. al., 2003). It is probably also fair to assume that the majority of people would consider surveillance as a means of ascertaining their intentions and predicting their behavior to be especially invasive.

6.1.5. Remote Sensing of Driver Posture and the Danger of Function Creep

Research in the UK has focused on the use of thermal infrared remote sensing for posture detection of drivers, purportedly as a means of developing safety systems (Amin, et. al., 2007). Using relatively inexpensive low-resolution thermal infrared sensors mounted inside a driving simulator, researchers found that based on algorithms formulated from thermal imagery, driver posture could be accurately discerned from remotely sensed data. The researchers suggest that because the imagery is low-resolution thermal infrared imagery, the technology is less intrusive and therefore ideal as the basis of a driver safety system which could, for instance, sound an alarm to awaken a drowsy driver. The researchers do acknowledge, however, that, "Simply linking the IR system with road speed, throttle, and braking information is straightforward and low cost and can provide a rich data source that can be used to identify high-risk situations or behaviours…" (Amin, et. al., 2007). While driver safety systems are clearly beneficial, the standard inclusion of a "black box" to monitor and record a driver's every move in the service of safety, could provide valuable information to other interested parties, including law enforcement agencies and insurance companies determining risk, setting premium costs, and evaluating claims. This clear example of possible "function creep", wherein a technology finds use in areas other than those for which it was purportedly designed, could be considered a threat to privacy, as well as a power shift detrimental to the driver (Amato, 2001).

6.1.6. The Orwell and Panopticon Metaphors

The spectre of unchecked proliferation in the use of remote sensing for surveillance in contemporary society naturally calls to mind Orwell's dystopian tale of the oppressiveness of life under pervasive government surveillance in a totalitarian regime. Analogies have also been drawn to Jeremy Bentham's circular prison design, the Panopticon, wherein prisoners who are watched from a central location cannot see their watchers. Nevertheless, the continuous possibility of being monitored alters the prisoners' behavior (Haggerty and Ericson, 2000).

6.2. Privacy and GIS

6.2.1. Reverse Geocoding

The extraction of the exact addresses of individuals through reverse geocoding is a privacy concern particularly with regard to health and criminal records and with regard to vulnerable members of populations, such as the elderly. Researchers at Louisiana State University describe their use of reverse geocoding, along with a map published in a local newspaper, to locate the addresses where Katrina victims' bodies were found (Curtis, et. al., 2006). Central coordinates for each body recovery location were extracted from oversized point symbols used on the map. The extracted locations were then checked using GPS and markings on the houses in New Orleans. The researchers were able to accurately extract the body recovery locations, in some cases exactly, and in all cases to within one or two houses. They point out that reliance on an oversized point symbol was entirely ineffective and question the ramifications of such practices in sensitive issues such as the mapping of HIV cases. They conclude, "Unless we in academia take the lead in expanding and enforcing a more rigid set of spatial display rules, especially for point data, we run the risk of an over-zealous tightening of data release and a protracted battle to again persuade those in power that a map can be used for the good of society"

(Curtis, et. al. 2006). Their concern for possible “over-zealous tightening” of rules appears unfounded based on the level of concern generally exhibited by the public and policymakers, alike. Nevertheless, although some may consider address extraction relative to body recovery locations somewhat inconsequential, the relative ease of extraction, along with the impossibility of determining how and by whom any extracted data is ultimately used, signals a significant danger to personal privacy.

6.2.2. Dataveillance

Prior to computerization, digitization, and networking, universal access to decentralized public records did not pose a significant privacy problem, since gathering data was extremely resource intensive. Privacy was reasonably well protected by existing laws, societal norms, and relative inefficiency (Nissenbaum, 1998). Subsequent technological advances have made large scale data acquisition and aggregation not just possible, but profitable as well. What has resulted is dataveillance, the systematic surveillance of personal data (Cho, 2008).

The Computer Matching and Privacy Protection Act of 1988 was intended to prohibit the merging of large databases of personal information, at least by government, and thereby prevent the collection of large amounts of personal data on individuals (Curry, 1997). The law, however, has been entirely ineffective due to the very nature of geodemographics, which allows for database merging not on the basis of personal identifiers, but through the use of geographic locators. Circumvention of the law allows the creation of quite accurate profiles of individuals, created not by merging data from government sources, but by geographically referencing publicly available data (Curry, 1997). According to Curry (1997), “Data matching statutes can, in principle, be effective as long as they are based on contingent markers, such as the social security number. But when we begin to use as an identifier geographical location, the world opens up.”

That new vista gives rise to privacy violations through data mining and data profiling, which effectively result in the stereotyping of entire neighborhoods or geographical groupings of people based on aggregation of data from linked databases. One commercially available "market segmentation system" is ESRI's *Community Tapestry*, the handbook for which reads:

> Segmentation explains customer diversity, simplifies marketing campaigns, describes lifestyle and lifestage, and incorporates a wide range of data. Segmentation systems operate on the theory that people with similar tastes, lifestyles, and behaviors seek others with the same tastes—"like seeks like." These behaviors can be measured, predicted, and targeted. ESRI's segmentation system, Community Tapestry, combines the "who" of lifestyle demography with the "where" of local neighborhood geography to create a model of various lifestyle classifications or segments of actual neighborhoods with addresses—distinct behavioral market segments. (ESRI, 2009)

Simply stated, Community Tapestry classifies US neighborhoods into 65 market segments based on socioeconomic and demographic composition. Descriptive and highly connotative names of the segments include, for example, Top Rung, Laptops and Lattes, Salt of the Earth, Las Casas, and Inner City Tenants (ESRI, 2009).

In addition to undermining personal privacy, profiling can lead to discriminatory practices against members of particular groups. For these reasons, profiling has been called unethical and potentially immoral by some. The broad generalizations of profiling naturally necessitate some error on the level of the individual. Dummer (2008) cautions, "Policy derived from geographic research can fall victim to ecological fallacy, in which incorrect assumptions are made about people based on aggregated data about their communities." Such stereotyping may perpetuate social and economic injustices, such as discriminatory lending practices and questionable public policy decision making.

According to Curry (1992), as of the early 1990s, National Decision Systems' EQUIS maintained "a database of financial information for over 100 million Americans on more than 340 characteristics, including age, marital status, residential relocation history, credit card activity, buying activity, credit relationships (by number and type), bankruptcies, and liens….updated continuously at a rate of over 15 million changes per day." Data aggregator companies such as ChoicePoint, LocatePlus, Seisint, LexisNexis, and Acxiom, currently collect, process, and store detailed data from both public and "unverified private sources" for the compilation of "millions of detailed records on individuals" which are sold to commercial and government entities (Holtzman, 2006). As previously indicated, individual level data which may be illegal for government agencies to collect and maintain based on the Privacy Act, are instead obtained through private sector contracts in, according to Holtzman (2006), an environment of "increasingly close connections between government and private-sector data-collection companies…."

The "unverified private sources" of data likely include transaction data, resulting from the routine conduct of personal business, which is then transferred to third parties despite implied protections in so-called privacy policies. Information is traded freely, seemingly without consequence. A case in point is the 2003 class-action lawsuit against JetBlue Airways for privacy violations resulting from the sale of 5 million customers' personal data to a Defense Department contractor. The suit was dismissed in 2005 based on the judge's ruling that although the sale of the data to a third party was a violation of the company's privacy policy, "there was no proof that damages resulted from the actions of the airline or that it 'unjustly enriched itself' from the sale of the data" (Holtzman, 2006). Unfortunately, there appear to be no provisions for compensating damages to society resulting from the erosion of consumer confidence in fair business and privacy practices. Equally alarming is the realization that, in addition to the inadequacies of the legal system, self-regulation is not working, either.

Another likely source of information for most data aggregators is tracking data furnished to websites knowingly or unknowingly by internet users. Nissenbaum (1998) cites this 1997 advertisement in the New York Times:

> With a 98% compliance rate, our registered users provide us with specific information about themselves, such as their age, income, gender and zip code. And because each and every one of our users have verifiable e-mail addresses, we know their data is accurate – far more accurate than any cookie-based counting. Plus, all of our user information is warehoused in a sophisticated database, so the information is stable, accessible and flexible….we can customize user groups and adjust messages to specific segments, using third-party data or additional user-supplied information. So you can expand your targeting possibilities. What's more, because they're New York Times on the Web subscribers, our users are affluent, influential and highly engaged in our site.

Privacy of information is often traded, both online and off, for perceived benefits, such as survey rewards, or participation in social networking sites, including MySpace, Facebook, Twitter, Flikr, etc. Whether or not individuals fully understand the extent to which they are exposing private information, once data is freely and openly provided without a reasonable expectation of privacy, it becomes part of the public domain, free to be collected, processed, and sold. Clearly, privacy has become a bargainable commodity at several levels. According to Haggerty and Ericson (2000), "Privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation where privacy is traded for products, better services or special deals."

6.2.3. Location-based Services (LBS)

Calling location-based services "an application of exciting potential which integrates nearly all aspects of Geographic Information Science, " Brimicombe (2008) glowingly describes the emerging technology in this way:

> Suppose all our wayfinding infrastructure for all forms of transport (including pedestrian) and for all forms of information was digital and accessible through an electronic mobile device, and anytime we wanted information tailored to where we were and what we were doing, all we would have to do would be to consult it. Suppose, further, that the in-built intelligence could tell us things we would like (or ought) to know even without being asked, just based on who we are, where we are, where we've been, and what time of day it is. Could we then get through the day without GIS? Welcome to the brave new future of location-based services! (Brimicombe, 2008)

The tone of Brimicombe's description contrasts sharply with the deep concern of others, especially Dobson and Fisher, who characterize the social hazards of tracking capabilities inherent in LBS as *Geoslavery*, warning that, "Like nuclear energy, LBS offers major benefits on the one hand and horrendous risks on the other" (Dobson and Fisher, 2003).

Referring to geoslavery, O'Sullivan notes that, "While the term…may seem alarmist, its use by two stalwarts of the GIScience community is thought-provoking." He calls the availability of individual tracking data, "a serious privacy and ethics issue for society as a whole, when even those working with GIS in tightly controlled academic settings are struggling to develop appropriate responses." He also points out the dearth of articles in GIScience journals addressing social or theoretical issues (O'Sullivan 2006).

Research, marketing, and application of location-based services are gaining momentum in the US. Location based services already routinely track the movement of goods, pets, prisoners, and sometimes employees, while encouraging us to also track loved ones. Often emphasizing safety benefits, tracking services are marketed under names like *Digital Angel* and *Travel Eyes* (Dobson and Fisher, 2003). One company offers multi-level service plans, ironically named, *Liberty, Independence, and Freedom* (Dobson, 2005).

6.2.4. Surveillant Assemblages and Data Doubles

Surveillant assemblage refers to a system wherein the data from a multiplicity of discrete surveillance systems is merged in myriad ways. Consider a GIS using a multitude of databases of personal information and add to it real time geographic tracking ability by means of GPS. The goal is to create portraits of individuals in an effort to capture behavioral characteristics. The resulting portrait of each individual can be thought of as a "data double," which can stand in for and represent individuals in ways which can be quantified and which are presumed to be predictable (Haggerty and Ericson, 2000). What results is the creation of "...a new type of individual, one comprised of pure information"

(Haggerty and Ericson, 2000). The ultimate goals of surveillant assemblages, generally unbeknownst to its subjects, are “control, governance, security, profit and entertainment” (Haggerty and Ericson, 2000).

Most alarming to privacy advocates is that the creation and use of surveillant assemblages are difficult and maybe even impossible to regulate, due to their malleable nature. They are changing constantly as they link new and different data pools collected through the use of discrete surveillance technologies. Defining what makes them legally objectionable may be impossible, since their use is so widespread and their construction results from mostly legally acquired building blocks (Haggerty and Ericson, 2000). The public is just now beginning to understand that profits are being made from the sale of their “data doubles”. The applications and consequences of surveillant assemblages will likely grow with the expansion and integration of information and surveillance technologies, making possible the regeneration of the lives of individuals based on data collected about “movements, consumption patterns, reading preferences, tastes in erotica, personal contact,” etc. (Haggerty and Ericson, 2000). Witness the practically instantaneous re-creation via surveillance data, of the movements and preferences of the terrorists immediately preceding 9/11.

6.2.5. The Kafka Metaphor

Solove (2008) suggests that current dataveillance practices are best described not by the Orwell metaphor of centralized surveillance resulting in inhibition and social control, but instead by what he calls the Kafka metaphor, based on *The Trial*, Franz Kafka’s novel about a man arrested and prosecuted for an unspecified crime. The protagonist lives in a bureaucratic society which not only controls data about its members, but also prohibits their access to it, creating an imbalance of power resulting in frustration and helplessness. Solove (2008), among others, believes we are facing a similar set of circumstances. We have lost control of information about ourselves. We do not know what data has been collected or by whom. In the absence of enforceable privacy protections, it appears we are helpless.

6.2.6. Fighting Back: Webcams and Extreme Blogging

An interesting twist to modern surveillance is the degree to which the watched are also watchers. Popular websites like Google earth offer frequently updated high resolution satellite imaging of most areas on earth. Camera equipped cell phones are everywhere. Live webcams from all over the world are available continuously on the internet. YouTube, founded in 2005 with the slogan, "Broadcast Yourself," reached 100 million US viewers by the end of 2008 (YouTube, 2009). And according to the Pew Internet and American Life Project, by the end of 2004 eight million Americans had blogs (Holtzman, 2006). The implications are that we are increasingly tolerant of surveillance, that we are complicit in our surveillance, and that surveillance often takes the form of entertainment.

In a study of online diaries, deLaat (2008) notes that most bloggers do not avail themselves of technical options for managing privacy, choosing instead to have their intimacies publicly accessible. He also suggests that our media experiences, as evidenced by the proliferation of reality and talk shows, are defined essentially by voyeurism and exhibitionism, and are "a perverse reaction to the erosion of privacy in the 20th century." According to deLaat, the "extimacy" or "intimacy turned inside out" practiced by online diarists is an attempt to create their own synopticism, defined, in contrast to panopticism, as the many watching the few. Like the Jennicam, maintained by lifecaster Jennifer Rigley from 1996 through 2003, extreme blogging is practiced by those attempting total transparency. It is interpreted by deLaat as a form of "empowering exhibitionism," a subversive attempt to return and nullify "the societal gaze of surveillance" (deLaat 2008).

6.3. Ancillary Technologies and the Trend towards Integration

6.3.1. Nano-technology and Radio Frequency Identification Systems

Radio Frequency Identification (RFID) technology is based on the use of inexpensive computer chips as small as 0.4mm square, which store unique EPCs (electronic product codes). The data is quantized to 96 bits enabling, according to Albrecht and McIntyre, authors of *Spychips*, "enough combinations of unique numbers to number every grain of sand on earth." Perhaps more specifically, they state that number to be "80 thousand trillion, trillion objects" (Albrecht and McIntyre, 2005). Ostensibly created as an improvement over UPCs for more efficient tracking of goods, EPCs have tiny antennas and are able to passively (and in some formats, actively) communicate their locations to sensors as small as a standard hardback book, from possibly as far as thirty feet away (Holtzman, 2006). Partially driven by merchandizing giant Wal-Mart, who is progressively mandating the use of the technology by its suppliers, the demand and use of RFID technology is predicted to expand rapidly (Holtzman, 2006). Juels (2006) predicts that, in response to diminishing costs, RFIDs "are likely to proliferate into the billions in the next several years – and eventually into the trillions." The tiny EPC's are already being planted in consumer goods, with plans to implant them in every manufactured or processed product, including food packaging. Already imbedded in the Euro as of 2005, implantation in U.S. currency may also be under consideration (Holtzman, 2006). With their size expected to eventually be reduced to that of a period on this page, widespread or universal implantation of the easily concealed devices in consumer goods signals the advent of potentially universal surveillance, wherein consumers can be tracked through their every electronic purchase and possibly eventually their every cash purchase. Unchecked by legal protections or legal technological advances negating their effectiveness, the implications of widespread RFID implementation are ominous (Holtzman, 2006).

One especially alarming application approved by the Food and Drug Administration is the Verichip, an implantable RFID, designed for human identification and offered by Applied Digital Solutions. Currently marketed for security access control and medical-record indexing, a GPS version of the Verichip, allowing the tracking of human beings to within a few centimeters anywhere in the world, is under development (Holtzman, 2006).

According to Van Den Hoven and Vermaas (2007), "RFID foreshadows what nano-electronics has in store for our privacy: invisible surveillance." They suggest that nano-electronics will essentially allow all materials and surfaces to assist in the collection, processing, storing, and transferring of data, thereby making surveillance ubiquitous.

6.3.2. The Ultimate Integration: The Worldwide Sensor Web

The "intelligent, virtual presence" of sensor webs is fast approaching (Delin and Jackson, 2001). Autonomous, collaborative, and reconfigurable clusters of miniature satellites forming sensor webs are the future of space remote sensing (Prescott et. al., 1999). Scientists envision their integration with earth based sensor webs mirroring those in space, creating a worldwide sensor web "in which users can query, as a single unit, vast quantities of data from thousands or even millions of widely distributed, heterogeneous sensors" (Gibbons, et. al., 2003). A realization of this vision, which can perhaps be considered the ultimate surveillant assemblage, gives rise to multiple privacy issues involving control, access, security, and regulation of data management. Researchers acknowledge that "Much of the data that the sensor web collects will be highly private…" (Balazinska, et. al., 2007).

6.4. Moore's Law

Enormously influential, both because of its predictive ability and because it has become a powerful self-fulfilling prophecy, Moore's Law and its impact are discussed in detail by Schaller (1997). The law is based on Gordon E. Moore's observation and quantification of the growth of semi-conductor technology. In 1965, he noted that the doubling of the density of components of integrated circuits was occurring at regular intervals and he predicted the indefinite continuation of that growth rate (Schaller, 1997). The amazing accuracy of Moore's Law is, according to Schaller, due in part to its role as a "technomantra", the repetition and belief of which continues to lead to its fulfillment. Schaller also suggests that "the demand for smart cards, smart watches, smart fuel injectors and smart toasters is insatiable" as is the demand for personal computers, which will continue to drive the semiconductor industry. Not surprisingly, Miller (2008) notes that, "The growth of computing power is widely expected to continue the exponential rate implied by Moore's Law for at least two or three more decades."

Moore's Law, therefore, also implies that the current rapid and unrelenting pace of development in geospatial and ancillary technologies will continue as well, likely accompanied by continuing, and possibly expanding risks to privacy.

6.5. Tenner's Revenge Theory

Notwithstanding many undeniable benefits of geospatial and ancillary technologies, applications must be thoughtfully designed and carefully implemented. Edward Tenner's *Why Things Bite Back: Technology and the Revenge of Unintended Consequences* reminds us that we cannot anticipate every possible consequence of a purposeful action (Tenner, 1997). Even Brimicombe's (2008) enthusiastic characterization of location-based services is accompanied by a caveat. Referring to Tenner's work, Brimicombe cautions:

> Tenner's… revenge theory of technological innovation means that new technologies never ultimately solve the problem for which they were designed without creating new ones along the way. What is more, the new problems tend to be shifted in space and time becoming more hidden and therefore dangerous. (Brimicombe, 2008)

Particularly in light of Moore's Law, Brimicombe's interpretation of Tenner's theory suggests there will likely be unanticipated outcomes related to the rapid ongoing development of geospatial and ancillary technologies.

6.6. Endnotes

ALBRECHT, K., MCINTYRE, L., 2005, *Spychips: How major corporations and government plan to track your every move with RFID*, Neslon Current, Nashville, p. 26.

AMATO, I., 2001, Big brother logs on. *Technology Review,* 104: 58-63.

AMIN, I.J., TAYLOR, A. J., PARKIN, R. M., 2007, Driver tracking and posture detection using low-resolution infrared sensing. *Journal of Automotive Engineering,* 221: 1079-1088.

ARMSTRONG, M., RUGGLES, A. J., 2005, Geographic information technologies and personal privacy. *Cartographica,* 40: 63-73.

BALAZINSKA, M., DESHPANDE, A., FRANKLIN, M. J., GIBBONS, P. B., GRAY, J., NATH, S., HANSEN, M., LIEHOLD, M., SZALAY, A., TAO, V., 2007, Data Management in the Worldwide Sensor Web. *Pervasive Computing*, (April-June): 10-20.

BRIMICOMBE, A. J., 2008, Location-based Services and Geographic Information Systems, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 581, 583, 588-590, 592, 594.

CHO, G. C. H., 2008, Geographic Information Science, Personal Privacy, and the Law, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 526-528.

CURRY, D. J., 1992, *The New Marketing Research Systems: How to Use Strategic Database Information for Better marketing Decisions*, John Wiley and Sons, New York, p. 264.

CURRY, M. R., 1997, Digital People, Digital Places: Rethinking Privacy in a World of Geographic Information. *Ethics & Behavior*, 7: 253-264.

CURTIS, A. J., MILLS, J. W., LEITNER, M., 2006, Spatial Confidentiality and GIS: reengineering mortality locations from published maps about Hurricane Katrina, *International Journal of Health Geographics*, 5: 44-56.

DE LAAT, P., 2008, Online diaries: reflections on trust, privacy, and exhibitionism. *Ethics and Information Technology,*10: 57-69.

DELIN , K. A., JACKSON, S. P., 2001, The Sensor Web: A New Instrument Concept. *Presented at SPIE's Symposium on Integrated Optics*, 20-26 January, San Jose, CA.

DOBSON, J. E., 2005. Every step you take, every move you make. *Chicago Tribune*, (February 25), [www.newsbank.com] accessed November 1, 2007.

DOBSON, J. E., FISHER, P. F., 2003, Geoslavery. *IEEE Technology and Society Magazine,* 22: 47-52.

DORITY, B., 2001, Big brother is watching! *Humanist,* 61: 9-13.

DUMMER, T. J. B., 2008, Health geography: supporting public health policy and planning. *Canadian Medical Association Journal*, 178: 1177-1180.

ESRI, [http://www.esri.com/library/brochures/pdfs/community-tapestry-handbook.pdf], accessed June 25, 2009.

GIBBONS, P. B., KARP, B., KE, Y., NATH, S., SESHAN, S., 2003, IrisNet: An Architecture for a Worldwide Sensor Web. *Pervasive Computing,* October-December: 22-32.

HAGGERTY, K. D., ERICSON, R. V., 2000, The surveillant assemblage. *British Journal of Sociology,* 51: 605-622.

HOLTZMAN, D. H., 2006, *Privacy Lost: How Technology is Endangering Your Privacy.* Jossey-Bass, San Francisco, pp. 8, 31, 93-117, 176-178.

JUELS, A., 2006, RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications,* 24: 381-394.

MILLER, H. J., 2008, Geographic Data Mining and Knowledge Discovery, in *The Handbook of Geographic Information Science*, eds. Wilson, J. P., Fotheringham, A. S., Blackwell Publishing, Malden, MA, pp. 352, 358.

NISSENBAUM, H., 1998, Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17: 559-596.

NIXON, M., CARTER, J. N., 2004, Advances in automatic gait recognition. Automatic Face and Gesture Recognition, 2004. Proceedings. Sixth IEEE International Conference on 17-19 May 2004, pp. 139-144.

O'SULLIVAN, D., 2006, Geographical information science: critical GIS. *Progress in Human Geography,* 30: 783-791.

PRABHAKAR, S., PANKANTI, S., JAIN, A. K., 2003, Biometric Recognition: Security and Privacy Concerns. *IEEE Computer Society. IEEE Security and Privacy, 2003,*pp. 33-42.

PRESCOTT, G. E., SMITH, S. A., MOE, K., 1999, Real-Time Information System Technology Challenges for NASA's Earth Science Enterprise. *Proceedings of the 20th IEEE Real-Time Systems Symposium, 1999*.

SCHALLER, R. R., 1997, Moore's Law: Past, Present, and Future.   *IEEE Spectrum*, July, pp. 52-59.

SOLOVE, D. J., 2007, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review,* 44: 745-772.

TENNER, E., 1996, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences.* Knopf, New York.

VAN DEN HOVEN, J., VERMAAS, P. E., 2007, Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon. *Journal of Medicine and Philosophy,* 32: 283-297

YOUTUBE, [http://www.youtube.com], accessed July 1, 2009.

Chapter 7

Discussion and Conclusions

7.1. Discussion

The capabilities of geospatial and ancillary technologies continue to expand at a rapid pace. Developments in remote sensing technology are marked by increasing spatial, spectral, radiometric, and temporal resolutions, along with the emergence of innovative and non-traditional applications. Furthermore, the miniaturization of satellites and the sensors they incorporate, offers greater flexibility and economic feasibility, as remote sensing technology trends towards constellations of smart satellites. Concurrently, GIS enjoys continued rapid expansion, nourished by computer and internet advances, a growing wealth of data products, and innovative ways of storing, processing, analyzing, and using those products. GIS also appears to be trending towards the application of spatialization concepts to traditionally non-geographic study areas, both abstract and concrete. Meanwhile, GPS capabilities, already central to traditional geospatial applications, continue to expand globally, just as ancillary technologies, most notably RFID and nano-technologies, continue their rapid advancement. At the same time, and perhaps most significantly, the overall trend in technology appears to be towards integration both within discrete technologies and among them. Integration and interoperability are necessary to reach several technological goals, including the expansion of location-based services and the creation of a geospatial semantic web and a grid of distributed, yet seamlessly integrated computing resources. The ultimate result could be the interconnection of earth-based and space-based sensor webs, forming a worldwide sensor web which, together with expanding biometric technologies and emerging RFID and nano-technologies, may signal the advent of both ubiquitous computing and ubiquitous surveillance capabilities.

At the same time, the effectiveness of the existing limited privacy protections in the United States continues to diminish. Amato (2001) quotes Barry Steinhardt of the ACLU as saying, “The technology is developing at the speed of light, but the privacy laws to protect us are back in the Stone Age.” The continued inadequacy of legal protections in the US appears to be driven by a number of factors, including powerful lobbying by corporations and government policing agencies, a general lack of awareness among the population, and a willful disregard on both the individual and societal levels of the importance of privacy protections.

7.2. Conclusions

While providing enormous benefits, geospatial and ancillary technologies are also posing significant risks, particularly in light of limited privacy protections. The expanding capabilities of geospatial and ancillary technologies, along with the integration of discrete technologies into surveillant assemblages, are impacting privacy in both predictable and unpredictable ways. In light of Moore’s Law and Tenner’s Revenge Theory, the momentum of technological change suggests that our ability to control the consequences of the applications of some geospatial and ancillary technologies may be both limited and diminishing. It appears there will likely be consequences unforeseen by researchers, policy and lawmakers, and the public at large. Some of those consequences will be auspicious, but some will not.

In general, the boundaries of privacy appear to be shifting, with the territory of privacy shrinking, partially as a result of technological change, but also due to legal and cultural changes. The tensions within government to protect the individual while protecting the society at large play a significant role. Those tensions are particularly evident with regard to US policymaking aimed at protecting economic prosperity and national security.

The effects of current and predicted future technological trends on the individual’s emotional, psychological, physical and spiritual wellbeing are as yet unknown. However, it is clear that the enormous benefits of geospatial and ancillary technologies may come at a cost to personal liberty. It is important to note that we are not just unwittingly contributing to our loss of privacy. As a society, we are also increasingly willing to trade privacy for real and/or perceived safety, for convenience, and for entertainment. In such transactions the point generally overlooked is that knowledge translates to power. The loss of control of personal information signals a boundary shift in both privacy and power relationships. The question now becomes, where is the boundary which, when crossed, signals the loss of autonomy?

We must assume that surveillance is here to stay, even if the metaphors for surveillance change as the practice of surveillance evolves. It seems clear that stronger legal, technological, and social protections are necessary. We need enforceable protective legislation, as well as readily available and easily implemented technological tools for protecting privacy. Furthermore, as a society, we need social norms that value privacy, as well as the will to protect it.

Finally, as an antidote to our complacency, we must acknowledge that, “Powerful forces work against any easy assumption that a decent society is self-perpetuating….There are no permanent victories in the liberties business.” (Marx, 2004).

7.3. Endnotes

AMATO, I., 2001, Big brother logs on. *Technology Review,* 104: 58-63.

MARX, G. T., 2004, What's New About the "New Surveillance"?: Classifying for Change and Continuity. *Knowledge, Technology & Policy*, 17: 18-38.

Vita

Lynn Brien was born in New Orleans, Louisiana and received her B.S. from Louisiana State University. After raising two sons with her husband, Kelly, she returned to the University of New Orleans to pursue her Master's degree in Geography.