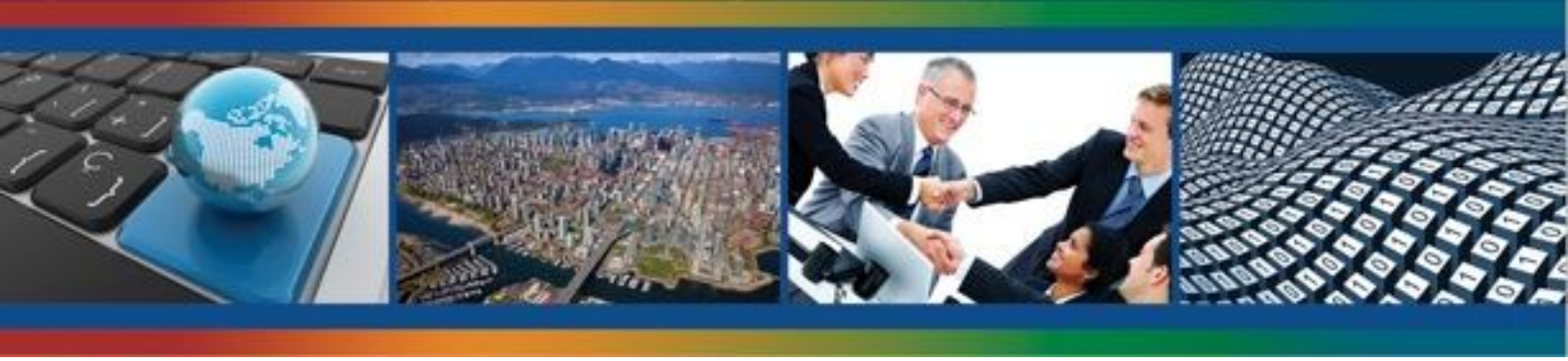

CANADIAN GEOSPATIAL DATA INFRASTRUCTURE
INFORMATION PRODUCT 12

Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies

Canada Privacy Services Incorporated

2010

Natural Resources Canada
Ressources naturelles Canada

Canada

Natural Resources Canada

Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies

March 31, 2010

Much geospatial information may appear, on its face, to be completely innocuous from a privacy perspective. Individual pieces of geospatial information may not allow for the identification of individuals. However, when that same geospatial data is combined with other information, it may become possible to identify individuals. This raises a number of complex questions regarding the point at which geospatial information becomes personal information for the purpose of privacy legislation.

(Lisa Madelon Campbell and Daniel Caron,
Office of the Privacy Commissioner of Canada, 2008)

Locational privacy is particularly challenging because much debate about privacy has traditionally been characterised in terms of who you are or what you are doing rather than where you are (and where you have been or where you are going).
(Caslon Analytics)

"Simply put, location changes everything. This one input – our coordinates – has the potential to change all the outputs. Where we shop, who we talk to, what we read, what we search for, where we go – they all change once we merge location and the Web."

(Mathew Honan, 2009)

Document Change Control Table

Version	Date	Description	Author
Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies	March 31, 2010	Client Final Version	CanadaPrivacy Services Inc.

Table of Contents

Document Change Control Table 1

Table Of Contents 2

Table Of Figures 4

Executive Summary 5

1. Introduction 8

1.1. About Geoconnections 8

In The Initial Phase Of Its Operations, Geoconnections Pursued Four Main Objectives: 8

2. Definitions & Acronyms 8

2.1. Definitions Table 8

2.2. Acronyms Table 12

3. Geospatial Information And Privacy 14

3.1. What Is Geospatial Information? 14

3.2. Geospatial Information In Canada: Background 14

3.3. Privacy Impact Of Geospatial Information 15

4. Legal & Policy Environments 17

4.1.1. The Privacy Act 17

4.1.1.1. Code Of Fair Information Practices 17

4.1.1.2. Other Privacy Act Requirements 20

4.1.2. The Personal Information Protection And Electronic Documents Act 21

4.1.3. Treasury Board Secretariat Of Canada Policies, Directives And Standards 21

4.1.3.1. Privacy Impact Assessment Policy 21

4.1.3.2. Standard On Geospatial Data 23

5. What Is Geospatial Personal Information? 24

5.1. The Statutory Environment 24

5.2. The Judicial Setting 27

5.2.1. Scope Of "Personal Information" 27

5.2.2. Meaning Of "Recorded" 28

5.2.3. Meaning Of "About" 28

5.2.4. Meaning Of "Identifiable" 31

5.2.5. Meaning Of "Individual" 31

5.2.6. When Does Non-Personal Geospatial Information Become Personal Information? 31

6. Geospatial Privacy Guidelines 33

6.1. Collection 33

6.2. Dissemination Of Personal Information 33

6.3. Privacy Breach Protocol 34

6.4. THE SEVEN "CS" OF GEOSPATIAL PRIVACY 35
6.4.1. Characterization *35*
6.4.2. Context *35*
6.4.3. Consultation *36*
6.4.4. Consistency *36*
6.4.5. Cumulative *36*
6.4.6. Caution *37*
6.4.7. Constraint *37*
7. Conclusion 38
8. Appendix A – Bibliography 39
8.1. PUBLICATIONS 39
8.2. CASE LAW 41
9. Appendix B – Geospatial Data Sets Inventory Report 43
Document Change Control Table 44
Table Of Contents 45
Executive Summary 47
10. Introduction 50
11. The Inventory Process 51
11.1. PHASE TWO: INVENTORY TOOL ADMINISTRATION 51
12. Tabular And Textual Compilation Of Inventory Results 51
12.1. MASTER LISTING OF DATA SETS BY INSTITUTION 51
12.2. CHARACTERIZATION OF INFORMATION 52
12.3. DATA SET MEDIUM/FORMAT AND VOLUME 54
12.4. ACCURACY OF RECORD GROUPS 55
12.5. SOURCE OF INFORMATION 56
12.6. AUTHORITY FOR DATA COLLECTION 57
12.7. PURPOSE OF DATA COLLECTION 57
12.8. MINIMIZATION AND ALTERNATIVES TO COLLECTION 58
12.9. USE AND DISCLOSURE OF INFORMATION 59
12.10. DATA SET DATABASE MANAGEMENT SYSTEM 60
12.11. DATA SET SECURITY FEATURES 60
12.12. DATA SET RETENTION AND DISPOSAL PRACTICES 61
12.13. RESPONDENT COMMENTS NOT CAPTURED ABOVE 62
12.14. DATA SOURCE STATISTICAL WRAP-UP 63
13. Appendix A – Listing Of All Participants 64

Table of Figures

Figure 1 - Definitions Table 12
Figure 2 - Acronyms Table 13
Figure 3 - TBS PIA Process Diagram 22
Figure 4 - Highlights of Inventory Findings 50
Figure 5 - Table of Geospatial Information Sources by Government Institution 52
Figure 6 - Table of Characterization of Information 54
Figure 7 - Table of Data Source Formats and Size 55
Figure 8 - Accuracy of Records in Record Group 56
Figure 9 – Source of Information 56
Figure 10 - Authority for Information Collection 57
Figure 11 - Purpose of Information Collection 58
Figure 12 - Data Collection Minimization 59
Figure 13 - Use and Disclosure of Information 59
Figure 14 - Data Source Management System 60
Figure 15 - Data Source Security Features 61
Figure 16 - Retention and Disposal Practices 62
Figure 17 - Respondent's Additional Comments 63

Executive Summary

GeoConnections is a national partnership program among federal, provincial and territorial governments, the private and academic sectors that is led by Natural Resources Canada (NRCan). Launched in 1999 with federal funding, this program was mandated to develop the policies, standards, technologies, and partnerships needed to build the Canadian Geospatial Data Infrastructure (CGDI), a one-stop, searchable Internet infrastructure for a wealth of location-based information. The CDGI is intended to provide a backbone for the sharing of location-based information throughout the country and across any number of jurisdictions.

One topic of particular concern to the GeoConnections partners is privacy. Working with guidance from the members of the Federal Government Geospatial Privacy Advisory Group, GeoConnections has developed this *Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies* ("Guide") to:

1. Define key terms that are of relevance to the issue of privacy in a geospatial context in Canada. In order for participants in the Canadian geomatics sector to engage in informed and constructive discussion regarding privacy in the context of this rapidly evolving area of activity, there must be a consensus regarding the meaning of some basic terminology. The Guide seeks to address this need by providing definitions for terms such as "geographic information", "geomatics" and "geospatial information".

2. Provide a brief background concerning the development of geospatial information in Canada. The Guide charts the exponential growth of geospatial data and applications in Canada during the last two decades, growth that has been facilitated and shaped by the ongoing involvement of the federal government in the development and dissemination of geospatial policies, standards and guidance documents.

3. Assess the privacy impacts of geospatial information in Canada. The report examines concerns that have arisen in this country, as they have elsewhere, about the potential for disparate streams of personal information being combined with (seemingly) non-identifying geospatial information in ways that may result in the development of very detailed profiles of individual behavior. These profiles, in turn, have the potential to be inimical to individual privacy.

4. Examine the legal and policy environments within which dealings with geospatial data by federal government institutions take place. The Guide briefly examines the *Privacy Act*, the *Privacy Regulations* and related Treasury Board of Canada Secretariat (TBS) policies and guidelines, and explores how they interact to establish a framework of rules governing the collection, use, retention, disclosure and disposal of personal information (and thus geospatial personal information).

5. Explore the meaning of "personal information" at law in Canada and assess whether the point(s) at which geospatial information becomes personal information can be accurately identified. Given the broad interpretation that the courts have given to the definition of personal information contained in the *Privacy Act*, and the elasticity of certain of the component elements of that definition ("...*"personal information" means information about an identifiable individual that is recorded in any form..."*), the

Guide posits that no clearly defined rule or standard can be applied to easily determine the point at which geospatial information becomes personal information. Rather, each data set or data element must be construed in its particular setting and circumstances, so as to determine whether it contains the necessary elements to attain, or avoid, "personal" status.

6. Furnish guidelines, including the *Seven "C's" of Geospatial Privacy*, for identifying and mitigating privacy-related risks and issues arising from the collection, use, retention, disclosure and disposition of personally identifiable geospatial information. The Seven "Cs" include:

   Characterization: The characterization of data as personal (or identifiable) information or non-personal (or non-identifiable) information is key to its proper treatment in a privacy law context. Determining the line of demarcation between the two types of information is not always straightforward and will sometimes require a subjective determination to be made that may prove to be controversial.

   Context: The context within which information occurs has a direct and important impact upon its interface with privacy law and policy. Individual data elements will, even when viewed in isolation, have a much higher likelihood of being characterized as being identifiable if they form part of a data set that is highly sensitive. The context within which information occurs also becomes important when the data set at issue is of a small size.

   Consultation: When in doubt - and sometimes even when not in doubt - consult! Given the uncertainties that can arise when attempting to characterize data elements as either personal or non-personal information or to properly deal with information that has been designated as being identifiable, federal officials would be well-advised to consult with other resources within their organization (or outside, if properly authorized) when confronted with such a task.

   Consistency: Each federal organization should make a concerted effort to ensure that it adopts a consistent approach to dealings with potentially identifiable geospatial information. To achieve this end, organizations should consider maintaining a centralized record of how data elements are characterized and treated in particular circumstances, with a view to replicating that treatment in future if identical or analogous conditions should exist.

   Cumulative: Geospatial data elements that are not identifiable when considered individually may become identifiable when combined with other data elements. This cumulative impact will vary depending upon the circumstances of each case, and thus will require fresh analysis each time that the circumstances and data elements change. As a general rule of thumb, the likelihood that data elements within a data set will combine to create a subset of identifiable data increases with each data element that is added to the subset. This is especially true if any of the data elements relate to a specific individual or to a specific location.

   Caution: "When in doubt, don't" is an appropriate initial approach to the issue of whether individual elements of geospatial data should be collected, used or released to third parties. This is not intended to recommend or support a reflexive refusal to deal with such data in all cases. Rather, it acknowledges the fact that issues surrounding privacy are complex and that caution should be exercised in cases where doubt exists.

   Constraint: When disseminating either identifiable or de-identified information to third parties, be sure to consider the merits of restricting the data recipient's rights via contract.

7. Communicate the results of an inventory of a sample of geospatial data sets held by federal government institutions. The inventory report is attached as Appendix B. In the course of conducting the inventory, a number of insights were obtained relating to the collection and dissemination of geospatial personal information, and to the need for institutions to implement viable data breach protocols. These insights are communicated in the report.

This guide is intended to provide officials of federal government agencies with assistance in making decisions related to the collection, use, disclosure and retention/disposition of geospatial personal information. While directed to the federal public sector, it is intended that the Guide be as general as possible so that it will be relevant to, and can be of utility to, the public, private, non-governmental organization ("NGO") and academic sectors.

1. Introduction

1.1.About GeoConnections

GeoConnections is a national partnership program led by Natural Resources Canada. Launched in 1999 with federal funding, this program was mandated to develop the policies, standards, technologies, and partnerships needed to build the Canadian Geospatial Data Infrastructure (CGDI), a one-stop, searchable Internet infrastructure for a wealth of location-based information. The CDGI is intended to provide a backbone for the sharing of location-based information throughout the country and across any number of jurisdictions.

In the initial phase of its operations, GeoConnections pursued four main objectives:

- first, to collaborate with provinces and territories in making Canada's location-based data more accessible and compatible;
- second, to collaborate with the private sector in developing technologies to share this data over the Internet;
- third, to create the partnerships and conditions required to build a national infrastructure; and
- fourth, to work with the public sector in developing the policies required to share data.

Now in its second phase of operations, which runs from 2005 through 2010, GeoConnections is working to ensure that decision-makers in key areas benefit from the CGDI. GeoConnections is seeking to accomplish this objective by co-funding projects that encourage key decision-making audiences (public health, public safety and security, the environment and sustainable development, and Aboriginal matters) to work with the Canadian geomatics sector in developing technologies that meet their specific needs.

2. Definitions & Acronyms

2.1.Definitions Table

Administrative Purpose	The *Privacy Act* defines an administrative purpose to mean, in relation to the use of personal information about an individual, the use of personal information in a decision making process that directly affects that individual.
Application	A program that performs a specific function directly for a user. Applications can make use of CGDI services.

Canadian Geospatial Data Infrastructure	An Internet/web infrastructure comprised of the developments of the federal, provincial, territorial and private sector partners who are creating the technology, standards, access systems and protocols necessary to harmonize all of Canada's geospatial databases, and make them available on the Internet.
GeoConnections	GeoConnections is a national partnership program among federal, provincial and territorial governments, the private and academic sectors that is led by Natural Resources Canada. Launched in 1999 with federal funding, this program was mandated to develop the policies, standards, technologies, and partnerships needed to build the Canadian Geospatial Data Infrastructure (CGDI), a one-stop, searchable portal for a wealth of location-based information. The CDGI is intended to provide a backbone for the sharing of location-based information throughout the country and across any number of jurisdictions.
Geoconnections Discovery Portal	A free online service that allows individuals and organizations to find geospatial data products and services. The GeoConnections Discovery Portal enables organizations to register and promote their data, services, resources and organization. The GeoConnections Discovery Portal is part of the CGDI and links to other parts of both the CGDI and other spatial data infrastructures.
Geographic Information	Any information that can be referenced geographically (i.e. that describes, or can be linked to, a location).
Geographic Information System	A computer system for capturing, storing, checking, integrating, manipulating, analyzing and displaying data related to positions on the earth's surface. A GIS can be used for handling various types of maps. These might be represented as several different layers where each layer holds data about a particular kind of feature. Each feature is linked to a position on the graphical image of a map, and layers of data are organized to be studied and to perform statistical analysis.
Geomatics	The science of gathering, analyzing, interpreting and distributing geographic information. Geomatics encompasses many disciplines that can be synthesized to create a detailed representation of the physical world and our place in it. These disciplines include surveying and mapping; remote sensing; geographic information systems; and global positioning systems**.**
Geospatial Data	Geospatial data is defined as data with implicit or explicit reference to a location relative to the Earth.
Global Positioning System	A satellite-based navigational system allowing the determination of a unique point on the Earth's surface with a high degree of accuracy given a suitable GPS receiver. The network of satellites is owned by the US Department of Defense.
Global Spatial Data Infrastructure	A global and open organization coordinating the organization, management and use of geospatial data and related activities. GSDI is being advanced through the leadership of many nations and organizations represented by a GSDI Steering Committee. This multinational Steering Committee includes representatives from all continents, and all sectors - government, academia, and the private sector. The "GSDI encompasses the policies, organizational remits, data, technologies, standards, delivery mechanisms, and financial and human resources necessary to ensure that those working at the global and regional scale are not impeded in meeting their objectives".

Info Source	A series of annual TBS publications in which federal government institutions are required to describe their institutions, program responsibilities and information holdings, including personal information banks (PIBs) and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the *Privacy Act*. Data-matching activities, use of the Social Insurance Number and all activities for which privacy impact assessments were conducted have to be cited in *Info Source* PIBs, as applicable. The *Info Source* publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Locational Privacy	Is the ability of an individual to move in public space with the expectation that under normal circumstances his or her location will not be systematically and secretly monitored.
Latitude and Longitude	Locations on the earth are defined using latitude and longitude. Longitude is a measure east-and-west relative to the Prime Meridian which runs through Greenwich, near London, in the United Kingdom. Latitude is a measure north-south relative to the Equator.
Personal Information	Personal information is defined in the *Privacy Act* to mean information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include (j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including, (i) the fact that the individual is or was an officer or employee of the government institution,

	(ii) the title, business address and telephone number of the individual, (iii) the classification, salary range and responsibilities of the position held by the individual, (iv) the name of the individual on a document prepared by the individual in the course of employment, and (v) the personal opinions or views of the individual given in the course of employment, (k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services, (l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and (m) information about an individual who has been dead for more than twenty years.
Personal Information Bank	A description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. Personal information described in a PIB has been used, is being used, or is available for use for an administrative purpose and is under the control of a government institution.
Portal	A web site considered as an entry point to other web sites, often by being or providing access to a search engine. The scope of a portal may be unlimited (such as Yahoo), or limited to a specific subject (such as geospatial information on the GeoConnections Discovery Portal).
Privacy	To the Office of the Privacy Commissioner of Canada (OPCC), privacy means *"…the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."*
Postal Code	Alphanumeric code assigned to groups of addresses by various national postal systems throughout the world to facilitate mail delivery. The Canadian Postal Code is a six-character uniformly structured, alphanumeric code in the form "ANA NAN" where "A" represents an alphabetic character and "N" represents a numeric character. A Postal Code is made up of two segments: "forward sortation area" and "local delivery unit."
Record	Any documentary material, regardless of medium or form.
Registry	A listing of the individual datasets, services or other things made available by an organization to CGDI users. There are two kinds of registries: a type registry (a listing of the different types or classes of things, such as services, components or events, which are recognized by CGDI services or applications), and an instance registry (a listing of the individual services, components, datasets or other things that comprise the CGDI or are relevant to its users. Instance registries are used to identify, locate and describe individual instances.)

Security	Security means reasonable precautions, including physical and technical protocols, to protect personal information from unauthorized collection, use, disclosure and access, and to ensure that the integrity of the information is properly safeguarded. A breach of security would occur whenever personal information is collected, used, disclosed or accessed other than as authorized, or its integrity is compromised.
Social Insurance Number	Is a number suitable for use as a file number or account number or for data-processing purposes, as defined in subsection 138(3) of the *Employment Insurance Act*. For the purposes of subsection 3(c) of the *Privacy Act*, the Social Insurance Number (SIN) is an identifying number, and is therefore considered to be personal information.
Spatial (Geospatial) Data Infrastructure	The relevant base collection of technologies, policies and institutional arrangements that facilitate the availability of and access to spatial data. A spatial data infrastructure provides a basis for spatial data discovery, evaluation and application for users and suppliers within all levels of government, the commercial sector, the non-profit sector, academia and citizens in general.
Vector	Data comprised of x-y coordinate representations of locations on the Earth that take the form of single points, strings of points (lines or arcs), or closed lines (polygons).
Web Map Service	An Internet-based service that allows clients to display maps and/or images with a geographic component and whose raw spatial data files reside on one or more remote WMS servers. The WMS conforms to the OpenGIS Web Map Server Interface specification.

Figure 1 - Definitions Table

2.2.Acronyms Table

CACS	Canadian Active Control System
CSRS	Canadian Spatial Reference System
GC	Government of Canada
GSM	Global System for Mobile Communications
LAC	Library and Archives Canada
LACA	Library and Archives of Canada Act
MOU	Memorandum of Understanding
N/A	Not Applicable

NAD 83	North America Datum, 1983
N/D	Not Determined
OECD	Organization for Economic Co-operation and Development
OPCC	Office of the Privacy Commissioner of Canada
PIB	Personal Information Bank
PGS	Policy on Government Security
PNAV	Precision Navigation, or Personal Navigation
PPP	Treasury Board, *Policy on Privacy Protection*
SIN	Social Insurance Number
SOS	Statement of Sensitivity
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment
XML	Extensible Markup Language

Figure 2 - Acronyms Table

3. Geospatial Information and Privacy

3.1. What is Geospatial Information?

Geospatial information is data derived from a variety of sources that contains precise geographic positioning information relative to the Earth's surface that is processed using common interoperable data standards. This type of information may include attribute data that describe the features found in the data set, such as a road network from a geographic information system (GIS), or a geo-referenced satellite image. Geospatial information is presented in a variety of formats: in print (e.g., a map or a publication), digitally (e.g., in a modeling database or as a digitized chart) or as a photograph or other digital image. It is also represented in a wide variety of scientific disciplines: geomagnetic, topographic, geodetic, aeronautical, hydrographic, toponymic, gravimetric, littoral, cultural and imagery (national source and commercial) data may all have geospatial aspects. The TBS *Standard of Geospatial Data* defines it as "*... data with implicit or explicit reference to a location relative to the Earth*."

3.2. Geospatial Information in Canada: Background

The impact of geospatial information on the daily lives of Canadians is growing exponentially. GPS-equipped smart phones and automobiles provide location-based services upon which consumers increasingly rely. Airlines and maritime shipping lines depend upon charts and other navigation aids that are now remarkably precise due to the incorporation of real-time positional data. Farmers and other agricultural sector businesses use geospatial data relating to soil composition and moisture content to conduct their operations. Municipalities utilize geospatial information to manage planning, utilities and emergency services. Innumerable private sector firms integrate geospatial information into the hardware and applications that they develop and sell.

These developments have been facilitated by an ever increasing volume of inexpensive (in some cases free) geospatial information that serves, in figurative terms, as grist for these new data mills. In some cases, the increased dissemination of this data is a result of developing business models amongst private sector firms (e.g., Google's mapping initiatives). In other cases, the data is being made available by governmental entities at various levels across Canada and abroad. Canada's federal government identified the sharing of geospatial information as a core policy priority a number of years ago; the *2001 Proposed Canadian Government Action Plan on Geospatial Data Policy* stated: "digital geospatial data that are collected by any level of government should be made as readily available electronically to the public as possible by improving access mechanisms and processes, unless there are privacy, security or competitive reasons not to do so." In 2009, TBS released its *Standard on Geospatial Data*. This Standard applies to all federal "departments" as defined in section 2 of the *Financial Administration Act* and defines "geospatial data" as being data with implicit or explicit reference to a location relative to the Earth. The Standard recognizes that geospatial data that is important to the social, economic and cultural well-being of Canadians is produced by federal, provincial and territorial governments and others. The Standard is intended to facilitate the sharing of information and to maximize the utility of existing mapping and related products. One of the expected results of the Standard is that geospatial information will be shared within and across departments to the greatest extent possible. Issues relating to the sharing of spatial

information have been further developed by GeoConnections, which released version 2 of *The Dissemination of Government Geographic Data in Canada: Guide to Best Practices* in 2008 GeoConnection's efforts in this area are ongoing; it released its *Best Practices for Sharing Sensitive Environmental Geospatial Data, Version 1* in March 2010.

Those activities that rely upon the processing of geospatial information share a common element: the manipulation of information that is specific to a particular geographic location. The significance of a particular location to the information compilation process will vary; for example, data relating to a position at which a particular smart phone call is made or received may be unique (and therefore quite limited) because the phone subscriber may change position with every call, whereas information relating to a fixed geographic point such as a road intersection may become voluminous over the course of time.

3.3. Privacy Impact of Geospatial Information

Concerns have arisen in Canada and elsewhere that the increasing utilization of geospatial data across all sectors is exacting a toll on individual privacy. The Assistant Privacy Commissioner of Canada stated in speeches on two occasions in 2009 that "Geospatial information is very much on our radar screen." The reasons for this concern have been canvassed extensively by popular and academic commentators - in essence, the potential for the combination of disparate streams of personal information with (seemingly) non-identifying geospatial information can result in the development of very detailed profiles of individual behavior. As noted by the Assistant Commissioner in a 2009 speech:

> *A lot of geospatial information may appear, on its face, to be completely innocuous from a privacy perspective. Individual pieces of geospatial information may not allow for the identification of individuals. However, when that same geospatial data is combined with other information, it may become possible to identify people.*
>
> *The ability to link data back to a particular person isn't always obvious.*
>
> *A few years ago, AOL published a list of 20 million web search queries and tried to protect the anonymity of users by assigning them with random numbers.*
>
> *The New York Times followed the data trail of clues in one of those user's search queries – 60 Year Old Single Men, Dog That Urinates on Everything, Landscapers in Lilburn, Georgia and so on – and quite easily identified "User No. 4417749" as a 62-year-old widow living in Georgia.*
>
> *Needless to say, this woman was shocked when a Times reporter called her up and was able to rhyme off three months worth of her search queries.*
>
> *More recently, a pair of U.S. researchers raised serious concerns that "anonymized" data collected from GPS-enabled devices may not be so anonymous after all. They found that knowing someone's approximate home and work locations to a block level can uniquely identify them.*

> *Indeed, the fact that, in many cases, we can attach supposedly anonymous information back to a particular person has spawned the creation of a new word in the English language – renonymize!*
>
> *Matching back "anonymous" data can be remarkably simple.*

Given this state of affairs, and given the legal obligations imposed upon federal government institutions by federal law and policy, it is incumbent upon users within the federal government community to ensure that their own dealings with geospatial information conform to applicable privacy standards. To facilitate such compliance, this Guide (i) examines the legal and policy environments within which federal institutions operate (in section 4 below), (ii) considers the manner in which de-identified information may become personal information (in section 5 below), and offers practical guidance on how users of geospatial information may avoid privacy-related pitfalls when dealing with geospatial information (in section 6 below).

4. Legal & Policy Environments

4.1.1. The Privacy Act

The *Privacy Act* provides Canadian citizens, permanent residents and all other persons present in Canada with (i) the right to access personal information held by federal government institutions, subject only to certain limited and specific exclusions and exemptions, and (ii) protection of that information against unauthorized collection, use, retention, disclosure and disposal. The Act's underlying principle is that individuals have a basic right to control their personal information; they have a right to know why their information is collected by the government, how it will be used, how long it will be kept and who will have access to it.

The *Privacy Act* also provides individuals with a basic right of access to all of their personal information held by federal government institutions, subject only to the limited and specific exclusions and exemptions described in that Act. Exemptions under the Act are either mandatory or discretionary. Decisions concerning the application of discretionary exemptions must be made in light of the basic right of access and the need for each government institution to be accountable to the public for its handling of personal information.

For the purposes of the *Privacy Act*, a "government institution" is (i) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule to that Act or (ii) any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*.

4.1.1.1. Code of Fair Information Practices

Sections 4-8 of the *Privacy Act* deal with the collection, accuracy, use, disclosure, retention and disposal of personal information. These sections are based on the internationally accepted standards for the handling of personal information which are contained in the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" adopted by the Organization for Economic Co-operation and Development (OECD) and accepted by Canada in 1984. Taken together, these sections of the Act constitute a "Code of Fair Information Practices".

Collection of Personal Information

The Act provides that government institutions shall not collect personal information unless it relates directly to an operating program or activity. Government policy requires that institutions have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. This means that each institution must have Parliamentary authority for the relevant program or activity, and a demonstrable need for each piece of personal information collected in order to carry out the program or activity.

The Act requires that, with very limited exceptions, institutions collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates. Exceptions to this rule arise in circumstances where:

- the individual has authorized indirect collection;
- the personal information was previously collected from the individual by another institution which is permitted to disclose the information by virtue of subsection 8(2) of the Act;
- the individual is deceased or incapacitated, cannot be located despite a reasonable effort, or is otherwise impossible;
- direct collection might:
  - result in the collection of inaccurate information; or
  - defeat the purpose or prejudice the use for which the information is collected.

The Act also provides that a government institution must inform any individual from whom the institution collects personal information about that individual of the purpose for which the information is being collected. An exception is available in circumstances where informing the individual would result in the collection of inaccurate or misleading information. Government policy has extended the Act's notice requirement by requiring that individuals who are asked to provide personal information (whether the information is about themselves or about someone else) must be informed:

- of the purpose of the collection;
- whether response is voluntary or required by law;
- of any possible consequences of refusing to respond;
- that the individual to whom the information pertains has rights of access to and protection of the personal information under the *Privacy Act*; and
- of the registration number of the Personal Information Bank (PIB) in which the information will be retained.

Consent

The *Privacy Act* does not prohibit non-consensual collection, use and disclosure of personal information. Instead, the Act focuses upon the issue of authority; if parliamentary authority exists for a particular dealing with personal information, then consent is not required. However, it is government policy that the consent of the individual should be requested, as a best policy, even in circumstances where the institution has the legal authority to use or disclose the personal information in question. The consent of the subject individual allows institutions to use or disclose personal information for any purpose consented to by that individual. Consent may be sought either at the time of collection of the information or subsequently, when a specific need arises. A consent should be in writing, signed (an electronic signature that meets the requirements of the *Common Look and Feel for the Internet* is acceptable when consent is being obtained via the Internet) and accompanied by a notice that contains the information required by government policy.

The *Privacy Regulations* provide that rights or actions under the *Privacy Act* and its regulations, including the giving of consent, may be exercised on behalf of a minor or a mentally incompetent individual by a person authorized by or pursuant to the laws of Canada or a province to manage the affairs of that individual. The *Privacy Regulations* further provide that rights or actions under the *Privacy Act* and its regulations, including the giving of consent, may be exercised on behalf of deceased persons by a person

authorized by or pursuant to the laws of Canada or a province to administer the estate of the deceased, but only for the purposes of such administration.

The provisions in the *Privacy Act* governing use and disclosure of personal information do not apply to information concerning an individual who has been dead for more than twenty years. Consent for the use or disclosure of information pertaining to individuals who have been dead less than twenty years should be sought from the executor or administrator of the individual's estate, and then only for the purpose of administering the estate.

Use of Personal Information

The *Privacy Act* provides that personal information may be used or disclosed by a government institution without the consent of the individual to whom it relates for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose. Such related purposes are termed "consistent uses". For a use or disclosure to be consistent, it must have a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. A test of whether a proposed use or disclosure is "consistent" may be whether it would be reasonable for the individual who provided the information to expect that it would be used in the proposed manner.

The *Privacy Act* requires Government institutions to publish, at least once each year, Personal Information Banks (PIBs) containing written descriptions of the primary purposes for which personal information in each PIB was obtained or compiled and descriptions of the consistent uses made of that information. The PIBs must be published in TBS' *Info Source* publication. The Act also requires that institutions notify the Privacy Commissioner whenever personal information is used or disclosed for a consistent purpose that is not identified in *Info Source*.

Personal information may also be used by a government institution without the consent of the individual to whom it relates for any purpose for which the information may be disclosed to that institution by another government institution pursuant to subsection 8(2) of the *Privacy Act*.

Disclosure of Personal Information

The *Privacy Act* describes the circumstances under which personal information under the control of a government institution may be disclosed without the consent of the individual to whom the information pertains. Such disclosures are discretionary and are subject to any other Act of Parliament.

The *Privacy Act* provides that the use and disclosure rules contained in sections 7 and 8 of the Act do not apply to personal information which is publicly available. This provision applies to information which has been published in any form or which constitutes or is part of a public record obtainable from another source. Although personal information which is publicly available is not protected by the *Privacy Act*, such information is still subject to all the remaining provisions of the Act. It must, for example, be processed in response to a request for access by the subject individual.

Retention and Disposal of Personal Information

Pursuant to the Act and the *Privacy Regulations*, personal information that has been used by a government institution for an administrative purpose must be retained by that government institution for at least two years following the last use of the information unless the individual consents to its earlier disposal. Where a request for access to personal information has been received, the institution shall

retain that information until such time as the individual has had the opportunity to exercise all of his or her rights under the Act.

Subject to the aforementioned retention requirements, the *Library and Archives of Canada Act* and government policy require each government institution to schedule its information holdings (including personal information) for retention and disposal. When personal information has surpassed its scheduled retention period and has been designated by the Librarian and Archivist of Canada as having archival or historical value, it must be transferred to the control of Library and Archives Canada; otherwise, it must be destroyed in a manner consistent with its security classification.

4.1.1.2. Other Privacy Act Requirements

Accuracy

The *Privacy Act* requires government institutions to take all reasonable steps to ensure that personal information that is used for an administrative purpose is as accurate, up-to-date and complete as possible.

Individual Access

The *Privacy Act* provides every individual who is a Canadian citizen or a permanent resident within the meaning of the *Immigration Act*, or who is present in Canada, a right of access to personal information about themselves that is under the control of a government institution. It is government policy that institutions should provide individuals with informal access to their personal information whenever possible. Government policy also requires institutions to endeavour to assist *individuals* in obtaining access to their personal information and in exercising their rights under the *Privacy Act*.

Right to Correction

The Act provides that every individual who is given access to personal information about himself or herself that has been used, is being used, or is available for use for an administrative purpose is entitled to request correction of the information where the individual believes there is an error or omission therein. The *Privacy Regulations* set out the procedures to be followed by an individuals seeking correction of their personal information and by government institutions responding to such requests.

Complaint Rights

Any Individual who feels that his or her Privacy has been violated by an Institution may complain to the Privacy Commissioner of Canada (PCC), who must investigate the complaint. The PCC has substantial powers to investigate a complaint, including the power to summon the appearance of persons before the Commissioner to give evidence, to administer oaths, to receive and accept evidence, to enter any premises occupied by an Institution, to converse in private with any person in those premises and to examine or obtain copies from books and other records found in those premises.

4.1.2. The Personal Information Protection and Electronic Documents Act

Private sector entities with which federal government institutions may exchange geospatial data are not subject to the *Privacy Act*. The federal law applicable to private sector dealings with personal information in Canada is called the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Care is needed in assessing the applicability of PIPEDA to any given transaction involving identifiable information, as PIPEDA is subordinated in some provinces (i.e., Quebec, Alberta, British Columbia) in some cases by provincial private sector privacy laws.

4.1.3. Treasury Board Secretariat of Canada Policies, Directives and Standards

The President of the Treasury Board is the Minister responsible for government-wide administration of the *Privacy Act*. While that Act and its associated Regulations establish formal legal rules for managing personal information, the Treasury Board of Canada Secretariat (TBS), which is responsible for providing federal institutions with guidance relating to the *Privacy Act* and its Regulations, has augmented those rules with numerous privacy-related policies, directives and standards. These include the *Policy on Privacy Protection* (PPP), the *Privacy Impact Assessment Policy*, the *Privacy Impact Assessment Guidelines*, the *Guidelines for Privacy Breaches* and the *Directive on Social Insurance Number*. In addition to these privacy-specific rule sets, TBS has developed security policies, information management policies and contracting policies that incorporate privacy considerations and compliment privacy management.

4.1.3.1. Privacy Impact Assessment Policy

TBS issued its *Privacy Impact Assessment Policy* (PIA Policy) and the related *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks* (PIA Guidelines) in 2002. The objective of the PIA Policy is

> *To assure Canadians that privacy principles are being taken into account when there are proposals for, and during the design, implementation and evolution of programs and services that raise privacy issues by;*
> - *prescribing the development and maintenance of Privacy Impact Assessments, and*
> - *routinely communicating the results to the OPC and the public*.

The PIA policy creates a systematic, principle-based consideration of the impact that a specific program or service will have on the privacy of an affected community. It is a risk identification and mitigation tool developed to facilitate project management and a process that ensures that privacy protection is a fundamental consideration in the initial framing, or revision, of programs or services. It integrates the privacy review with institutionally-specific laws and other federal laws; for example, the *Library and Archives of Canada Act*.

PIAs help to:

- reduce the risk of having to retract or rethink a program or service after it is launched;
- reduce the risk of causing client/partner confusion and diminished credibility;

- avoid development of programs and services that are not compliant with the *Privacy Act*;
- provide documentation on the business process and flow of personal information; and
- promote awareness and understanding of privacy issues.

PIAs are commonly undertaken when government initiatives involve:

- a new or increased collection, use or disclosure of personal information;
- a broadening of target populations;
- an increasing volume of personal information collected;
- new data sharing internally or externally;
- changes in electronic manipulation of data that affects personal information;
- new contracting with service providers involving personal information;
- alterations to security measures that may affect protection of personal information; or
- new programs that affect the use and disclosure of personal information.

According to the PIA Policy, the process required to undertake a PIA includes:

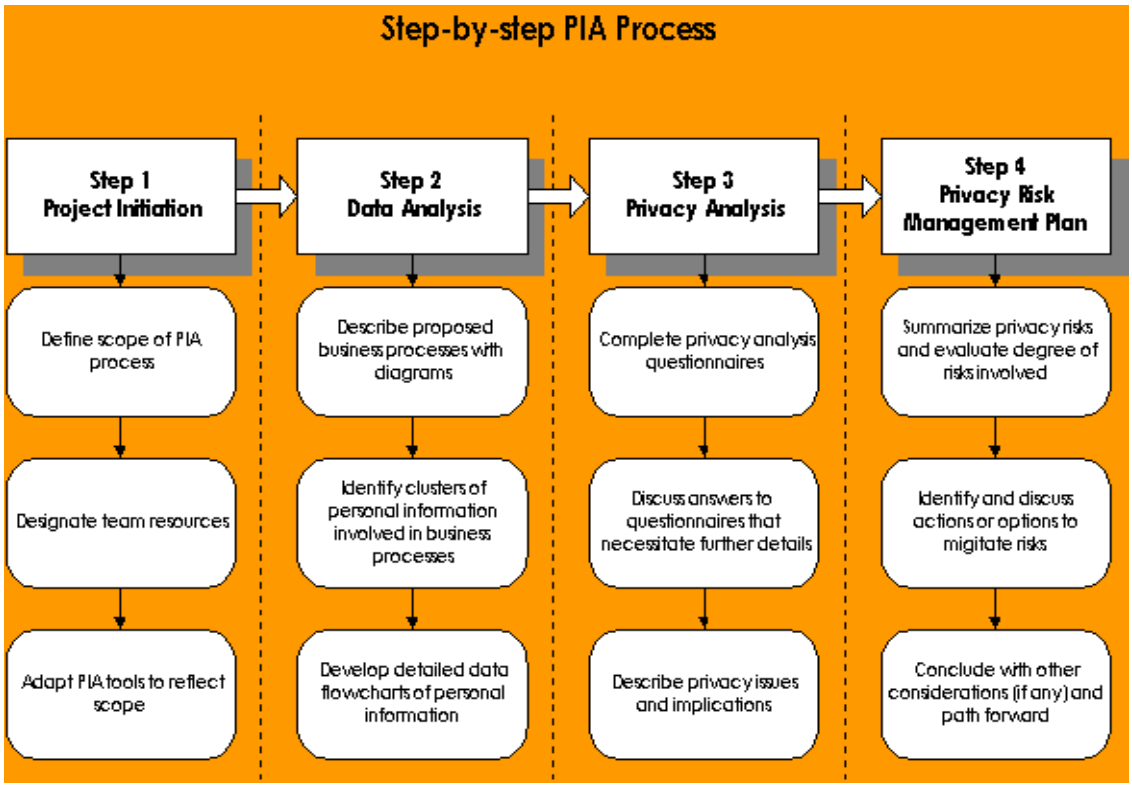

Figure 3 - TBS PIA Process Diagram

TBS has indicated that the PIA Policy and PIA Guidelines will undergo significant amendments during 2010.

4.1.3.2. Standard on Geospatial Data

TBS issued a *Standard on Geospatial Data* in June, 2009. This Standard applies to all federal "departments" as defined in section 2 of the *Financial Administration Act* and defines "geospatial data" as being data with implicit or explicit reference to a location relative to the Earth. The Standard recognizes that geospatial data that is important to the social, economic and cultural well-being of Canadians is produced by federal, provincial and territorial governments and others. The Standard is intended to facilitate the sharing of data and to maximize the utility of existing mapping and related products. One of the expected results of the Standard is that geospatial data will be shared within and across departments to the greatest extent possible. While the Standard is to be read in conjunction with the TBS *Policy on Information Management*, which contains references to requirements based in the *Privacy Act* related to the collection, use, disclosure and retention of personal information, the Standard makes no reference to privacy protection within the context of the sharing of geospatial data.

5. What is Geospatial Personal Information?

When endeavouring to apply Canada's federal privacy rules in the geospatial realm, a basic threshold issue arises: at what point does non-personal geospatial information (also frequently referred to as non-identifying and/or de-identified information) become personal information that is subject to the constraints imposed by statute, regulation and policy? To answer this question, it is first necessary to consider the statutory and judicial contexts within which federal government institutions interact with personal information.

5.1. The Statutory Environment

Every federal government institution[1] is subject to the restrictions on dealings with personal information contained in the *Privacy Act*. The Act provides Canadian citizens, permanent residents and all other persons present in Canada[2] with (i) the right to access personal information held by government institutions, subject only to certain limited exclusions and exemptions, and (ii) protection of that information against unauthorized collection, use, retention, disclosure and disposal. The Act's underlying principle is that individuals have a basic right to control their personal information; in this respect, they have a right to know why their information is collected by the government, how it will be used, how long it will be kept and who will have access to it.

"Personal information" is defined in section 3 of the *Privacy Act* in the following manner:

"Personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,
(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
(c) any identifying number, symbol or other particular assigned to the individual,
(d) the address, fingerprints or blood type of the individual,

[1] "Government institution" is defined in the *Privacy Act* to mean:
(*a*) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule [appended to that Act], and
(*b*) any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*.

[2] The class of individuals that enjoy rights under the *Privacy Act is established by the Order Extending the Right to Be Given Access to Personal Information Under Subsection 12(1) of The Privacy Act* (SOR/83-553) and the *Order Extending the Right to Be Given Access to Personal Information Under Subsection 12(1) of The Privacy Act* (SOR/89-206).

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,
(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,
(g) the views or opinions of another individual about the individual,
(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and
(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include
(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

> *(i) the fact that the individual is or was an officer or employee of the government institution,*
> *(ii) the title, business address and telephone number of the individual,*
> *(iii) the classification, salary range and responsibilities of the position held by the individual,*
> *(iv) the name of the individual on a document prepared by the individual in the course of employment, and*
> *(v) the personal opinions or views of the individual given in the course of employment,*

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and
(m) information about an individual who has been dead for more than twenty years.[3]

Treasury Board of Canada Secretariat's (TBS') 1993 *Privacy and Data Protection Guidelines - General* provide a somewhat dated, but still useful, synopsis of the federal government's own interpretation of this definition:

> *This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing", prior to the list of examples. Information which is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual". Additional examples of personal information would include information about an individual's sexual preference, income or political affiliation.*

---

3 Privacy Act, s. 3.

> *Paragraphs (j), (k), (l) and (m) of the definition place certain limitations on the definition of personal information for the purposes of the restrictions on use and disclosure contained in sections 7 and 8, the exemption provision contained in section 26, and the exemption contained in section 19 of the Access to Information Act. Therefore, information concerning the position or functions of a government employee (j); information about the services performed by an individual under contract for a government institution (k); information about a discretionary benefit of a financial nature (l); and information about an individual who has been deceased for more than twenty years (m) are not protected by the use and disclosure provisions of the Act.*
>
> *The limitations in paragraphs (j), (k) and (l) reflect the principle that the government's accountability to the public means that the public should have access to certain information concerning the public service, government contracts for services and the government's granting of discretionary financial benefits. The exclusions in these paragraphs should be interpreted narrowly, bearing in mind the Act's purpose to protect privacy. Thus these paragraphs should be applied to factual information related to the position, the contract or the discretionary benefit only. Assessments of an individual's job performance, conflict of interest declarations, or reports of disciplinary actions relate to the individual, not to the position, and would therefore not be included in the exception. The granting of a license or permit has to be discretionary and must confer a direct financial benefit on the individual in order to be removed from the protection of the Act. The granting of a license or permit is not considered discretionary if everyone who satisfies a set of objective requirements is given the license or permit, or if those who will receive the license or permit are determined by some other objective means, such as a lottery system.*
>
> *The limitation in paragraph (m) reflects the concept that the privacy interest declines with time after the death of an individual.*

Based upon the generality of the opening phrase in the definition of personal information ("...*information about an identifiable individual that is recorded in any form...*"), it is apparent that the term encompasses a potentially very large amount of information. Subject to the specific exceptions cited in the definition, all that is required for information to qualify as personal information is that it be (i) recorded in any form and (ii) be about an identifiable individual. In addition, to be subject to the rules governing personal information contained in the *Privacy Act*, information must not fall within the exclusions found in sections 68 through 70.1 of that Act. Certain of these exclusions may be relevant in the geospatial context, including those relating to:

- library or museum material preserved solely for public reference or exhibition purposes;[4]
- material placed in the Library and Archives of Canada, the National Gallery of Canada, the Canadian Museum of Civilization, the Canadian Museum of Nature, the National Museum of Science and Technology or the Canadian Museum for Human Rights by or on behalf of persons or organizations other than government institutions;[5]

---

4 *Privacy Act*, ss. 69(1)(a).

5 *Privacy Act*, ss. 69(1)(b).

- the use and disclosure of personal information that is publicly available;[6]
- personal information that the Canadian Broadcasting Corporation collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose;[7] and
- confidences of the Queen's Privy Council for Canada.[8]

5.2. The Judicial Setting

Unfortunately, the terms "recorded", "about", "identifiable" and "individual" are not further defined in the *Privacy Act* or in TBS policy. Nevertheless, decisions handed down by Canadian courts in the nearly three decades since the *Privacy Act* came into force have helped to refine our understanding of those terms as component elements of the term "personal information". Taken together, those decisions provide an invaluable guide to the parameters of personal information in the federal public sector environment as they pertain to geospatial data. A brief consideration of their most salient features follows.

5.2.1. Scope of "Personal Information"

The Supreme Court of Canada (SCC) has, on a number of occasions, held that "personal information" should be interpreted very broadly.[9] The Court has ruled that the list of examples in paragraphs (a) through (i) of the definition of that term should not be construed as limiting in any way the breadth of the introductory phrase "...*information about an identifiable individual that is recorded in any form...*".[10] Rather, the Court has held that the definition was intended by Parliament to capture any recorded information about a specific person, subject only to the specific exceptions listed in paragraphs (j) through (m) of the definition.[11]

---

6 *Privacy Act*, ss. 69(2).

7 *Privacy Act*, s. 69.1.

8 *Privacy Act*, ss. 70(a).

9 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 at para. 68; *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, 2002 SCC 53 at para 26; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, 2003 SCC 8 at para. 23.

10 *Dagg*, *supra*.

11 *Dagg*, *supra*, para. 69.

It is also possible that information concerning a group of persons can be attributed to each member of that group if the grouping is small enough (e.g., five or fewer members).[12] So, for example, information about the activities of a household that is not specific to individual householder behaviour may, nonetheless, still constitute personal information of each of the household members because of the small sampling size.

5.2.2. Meaning of "Recorded"

While the term "recorded" is not defined in the *Privacy Act*, a definition for the term "record" is found in the federal *Access to Information Act*: "*...'record' means any documentary material, regardless of medium or form*." As the SCC has held on more than one occasion that the *Privacy Act* and the *Access to Information Act* must be read together as a "seamless code",[13] it is appropriate to apply the *Access to Information Act* definition to the interpretation of the *Privacy Act*. Viewed in that light, personal information can be properly understood to exist in a wide variety of recorded formats, such as books, maps, drawings, photographs, sound recordings, and videotapes.[14] In addition, the SCC has stated: "*the Access Act clearly envisions a "record" as a "set" of information which can be divided or severed. For example, a book may include many discrete and severable "pieces" of information...*"[15]

5.2.3. Meaning of "About"

Recently, the Federal Court of Appeal has placed what appears to be a significant limitation upon the ambit of the term "personal information". In *Information Commissioner of Canada v. Canadian Transportation Accident Investigation and Safety Board*, the Court held that "'*personal information' must ... be understood as equivalent to information falling within the individual's right of privacy.*"[16] In that case, the Court examined the historical underpinnings of the *Privacy Act* before advancing its own "privacy-based interpretation" of the term "personal information". It held that information that was merely linked to an identifiable individual - in that particular case air traffic control communications between aircrew and an air traffic controller relating to the safety and navigation of aircraft, the general operation of the aircraft

---

12 *Montana Band of Indians v. Canada (Minister of Indian Affairs & Northern Development)*, [1989] 1 F.C. 143 (1988) at para. 21.

13 *Canada (Information Commissioner) v. Royal Canadian Mounted Police Commissioner*, [2003] 1 S.C.R. 66, 2003 SCC 8 (S.C.C.), at para. 22; *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] 1 S.C.R. 441, 2006 SCC 13(S.C.C.), at para. 2.

14 *Heinz*, *supra*, at para. 43.

15 *Heinz*, *ibid*.

16 2006 FCA 157 at para. 43.

and the exchange of messages on behalf of the public - was not personal information for the purposes of the *Privacy Act* because it was not "about" an individual in a way that that engaged the right to privacy. The Court noted:

> *The information contained in the records at issue is of a professional and non-personal nature. The information may have the effect of permitting or leading to the identification of a person. It may assist in a determination as to how he or she has performed his or her task in a given situation. But the information does not thereby qualify as personal information. It is not about an individual, considering that it does not match the concept of "privacy" and the values that concept is meant to protect. It is non-personal information transmitted by an individual in job-related circumstances.*[17]

The Court went on to add:

> The ATC communications, *when combined with other information*, may well in certain circumstances be *used* as a basis for an evaluation of their authors' performances. However, the possibility of such eventual use cannot transform the communications themselves into personal information, when the information contained therein has no personal content. [emphasis added]

In 2007, the SCC refused to hear an appeal of the Federal Court of Appeal's decision in the Air Traffic matter,[18] effectively rendering it the near equivalent of a SCC ruling and confirming the requirement for a "right to privacy" analysis when assessing the status of information attributable to a specific individual.

In 2008, the Federal Court considered the meaning of "about" in a decision by Gibson J. in *Gordon v. Canada (Minister of Health)*.[19] That cased revolved around the characterization of certain data elements contained in a Health Canada database called the Canadian Adverse Drug Reaction Information System (CADRIS). A newspaper had requested access to Adverse Drug Reaction data in electronic format pursuant to the *Access to Information Act*, but was refused access to a portion of the requested information on the basis that the data elements constituted personal information and were thus exempt from disclosure pursuant to subsection 19(1) of the *Access to Information Act*. Following the intervention of the Access to Information Commissioner, the data elements in dispute were reduced to one - the province field that indicated the province in which a particular Adverse Event Report had been produced. In court, the Applicant took the position that the province field data was not personal information because disseminating it would not allow for the identification of an individual, thereby bringing that data field within the definition of personal information in section 3 of the *Privacy Act*.
In rendering its decision, the Court referred to the ruling of the Federal Court of Appeal in the CTAISB case, in which the Court had stated:

---

17 *Ibid*, para. 54.

18 *Information Commissioner of Canada v. Canadian Transportation Accident Investigation & Safety Board* (2007**),** 368 N.R. 396 (note).

19 (2008), 2008 FC 258.

> *These two words, "about" and "concernant" [the French language equivalent of "about" in section 3 of the Privacy Act], shed little light on the precise nature of the information which relates to the individual, except to say that information recorded in any form is relevant if it is "about" an individual and if it permits or leads to the possible identification of the individual.*[20] [citations omitted, emphasis added]

The Federal Court in *Gordon* applied this reasoning and concluded that:

> *...information recorded in any form is information "about" a particular individual if it "permits" or "leads" to the possible identification of the individual, whether alone or when combined with information from sources "otherwise available" including sources publicly available.*
> *Counsel for the Privacy Commissioner, the Intervener, urged the adoption of the following test in determining when information is about an identifiable individual:*
>
> *Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.*
>
> *I am satisfied that the foregoing is an appropriate statement of the applicable text.*[21]

The Court noted that even in the absence of the province field data, the news media had been able to use information from other CADRIS fields that had been previously disclosed to identify an individual in British Columbia who had died from an adverse drug event.[22] The Court went on to note that it was satisfied that the provincial field of data, if combined with other data available to the Applicant/Requestor (i.e., other CADRIS data elements) would create a serious possibility that individuals could be identified through the use of that information. Consequently, the Court held that the information was personal information because it was "about" an identifiable individual.[23]

It is noteworthy that the parties in *Gordon*, with the Information Commissioner's approval, agreed prior to trial that certain other CADRIS data fields were personal information and could not be released. These included: ethnic group; notifier clinic (i.e., the health care facility that filed the adverse event report after dealing with the affected individual); notifier hospital; notifier name; notifier city; notifier phone number; patient initials; patient identifier; date of birth; date of conception; and date of death. Conversely, Health Canada ultimately agreed to the pre-trial release of three data fields that it had initially declined to release - year of death, year of birth and year of conception - on the basis that they were not personal information.[24]

---

20 *Information Commissioner of Canada v. Canadian Transportation Accident Investigation and Safety Board*, *supra*, para. 43**.**

21 *Gordon*, *supra*, paras. 33-34.

22 *Ibid*, para. 39.

23 *Ibid*, para. 43.

24 *Ibid*, para. 8.

It is even more noteworthy that the Federal Court's interpretation of the term "about" in *Gordon*, while stated to be made in reliance upon the Federal Court of Appeal's CTAISB decision, may diverge in at least one significant respect from the interpretation found in the higher court ruling. In *Gordon*, the Federal Court held that the possibility of data elements being combined to make an individual identifiable was sufficient to render those elements "about" the individual and, therefore, into personal information. In the Federal Court of Appeal's CTAISB ruling, the mere fact that a data element might result in identifiability was not deemed sufficient to make the element either "about" the individual or into personal information. Rather, what was required was the presence of a more amorphous element - one that triggers the right to privacy by being "about" the individual.

5.2.4. Meaning of "Identifiable"

In the Federal Court of Appeal's decision in *Information Commissioner of Canada v. Canadian Transportation Accident Investigation and Safety Board*, The Court Stated**:**

> *There is judicial authority holding that an "identifiable" individual is considered to be someone whom it is reasonable to expect can be identified from the information in issue when combined with information from sources otherwise available (Colin H. H. McNairn and Christopher D. Woodbury, Government Information: Access and Privacy (Toronto: Carswell, 1992) at p. 7-5; Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner) (2001), 154 O.A.C. 97 (Ont. Div. Ct.), aff'd (2002), 166 O.A.C. 88 (Ont. C.A.)).*[25]

5.2.5. Meaning of "Individual"

It is established in Canadian law that an "individual" for the purposes of the *Privacy Act* definition of personal information must be a human being (i.e.; not a corporation or other form of entity).[26]

5.2.6. When does Non-personal Geospatial Information become Personal Information?

Based upon the foregoing statutory and judicial analysis, it appears evident that no clearly defined rule or standard can be applied to easily determine the point at which geospatial information becomes personal information. Rather, each data set or data element must be construed in its particular setting and circumstances, so as to determine whether it contains the necessary elements to attain, or avoid, "personal" status.

---

25 *Information Commissioner of Canada v. Canadian Transportation Accident Investigation and Safety Board*, *supra*, para. 43.

26 *Tridel Corp. v. Canada Mortgage & Housing Corp.* (1996), 115 F.T.R. 185 (F.C.T.D.) at para. 23.

For example, it is established in Canadian law that information must be recorded in some format in order to be personal information. This distinction may be relevant in circumstances where geospatial data is "streamed" or transmitted in a "live" manner without being retained in a data storage system. Information that falls within any of the exceptions cited in section 3 of the *Privacy Act* or exclusions cited in sections 69 - 70.1 of that Act is not personal. Similarly, information concerning a non-human entity (e.g., a corporation) is not personal information, although this analysis may be complicated if the group of human beings that comprise the entity (e.g., a small partnership) is quite small.

The particular nature of information is not always determinative of whether it may constitute personal information. As demonstrated by the *Gordon* decision, a seemingly non-personal data field like "province" can easily become personal when combined with other data elements. Conversely, as demonstrated by the Federal Court of Appeal's CTAISB ruling, information that may permit the identification of an individual and pertains to that individual's behaviour (in that case job performance), may not be personal information because the nature of the information does not engage the right to privacy that underlies the *Privacy Act*.

6. Geospatial Privacy Guidelines

In addition to considering the need to conduct a privacy impact assessment associated with a geospatial program or service, government institutions that deal with geospatial information should consider the following guidelines as part of their privacy-related compliance programs. These have been derived through a review of the available literature and through insights obtained by conducting a sample inventory of federal geospatial data sets, a report of which is attached as Appendix B.

6.1. Collection

Prior to the collection of a data set, organizations should consider the following:

- Could the data set that your organization plans to collect contain identifiable information? If in doubt, consult with your organization's privacy and/or ATIP experts.

- If personal information elements are present or potentially present, is the collection of identifiable information required for your purposes? Remember that the *Privacy Act* (s. 4) obliges institutions to possess statutory authority for any collections of personal information.

- If the information is required, is there a means of minimizing the elements of personal information your organization will be collecting or compiling? Remember that government policy obliges government institutions to collect no more personal information than is required to meet their authorized and legitimate purposes.
-
    - Has consideration been given to the possibility of enlarging the geographic population references (e.g. block size) so as to reduce the identifiability of the information?

- Has the provider of the data set shown that it had the consent of individuals involved for disclosure of the data set to you? While consent is not a requirement of the *Privacy Act*, it is mandated by government policy whenever it is possible to obtain.

- Have you documented your decision to collect or not collect identifiable information, in order to facilitate subsequent review and/or audit?
- If your organization is receiving geospatial personal information, does the information sharing agreement contain provisions that are technologically challenging? Is your organization capable of fulfilling the obligations and passing an audit?

6.2. Dissemination of Personal Information

Prior to publishing or disseminating geospatial data that may contain elements that can be combined with externally sourced information to form personal information, organizations should consider:

- Has the geospatial information that your organization will be disseminating (e.g., specific addresses or location/movement information) been identified and documented?
- Has consideration been given to suppressing data elements in the data set to increase the likelihood that the information is non-identifiable?
- Has consideration been given to elevating the geographic area to a larger population size so as to reduce the identifiability of the information?
- Has an assessment been made concerning the possibility that downstream recipients of the geospatial information could re-identify the information that your organization will be disseminating? If this seems reasonably possible, the information should be treated as being personal information for the purposes of assessing your organization's entitlement to disclose.
- Can the geospatial information be disseminated or published in a manner that prevents that information from being geo-referenced? For example, can a map be re-created without geo-references in a .pdf format ? Remember, the goal should be to avoid the possibility of disseminating identifiable information other than in those cases where proper authority for such a disclosure exists.
- Has your organization documented its decision to disclose the data in a manner that will facilitate appropriate review and/or audit?
- Does your organization deal with substantial volumes of geospatial personal information and, if so, does it require a geospatial data management review structure?
- Are there other technological privacy risk mitigations, such as image blurring, that can be applied to the data set being disseminated to eliminate the risk of unauthorized disclosure of personal information?
- If your organization plans to disclose a data set with geospatial identifiers (e.g., telephone numbers, street addresses, household name(s), etc.) has an information sharing agreement been prepared that sets out how the recipient may use, retain, disclose and ultimately dispose of that information?

6.3. Privacy Breach Protocol

Every federal institution should ensure that it has the capability to respond to a privacy breach, should one occur.

- Has your organization established a terms of reference that inhibits downstream recipients of your public geospatial information from overlaying that information with other geospatial data, thereby potentially creating geospatial personal information? If information is made identifiable without authorization through combination with other data, a privacy breach has occurred. Any data sharing agreement should specify the limits that are imposed on downstream information use and make provision for periodic reviews or audits to confirm compliance.
- How would your organization respond to a privacy breach caused by an external party that involved your publicly available geospatial data? Does your organization have a privacy breach protocol that would address a privacy breach in a manner that is consistent with the TBS *Guidelines for Privacy Breaches* issued in 2007?

6.4. The Seven "Cs" of Geospatial Privacy

6.4.1. Characterization

The characterization of data as personal (or identifiable) information or non-personal (or non-identifiable) information is key to its proper treatment in a privacy law context. However, as discussed in section 5 above, determining the line of demarcation between the two types of information is not always straightforward and will sometimes require a subjective determination to be made that may prove to be controversial. Given this possibility, it would be prudent for each federal organization to briefly record and then retain its reasons for characterizing each data element as personal or non-personal. Ideally, each such characterization should be capable of being supported in an objective manner, through recourse to demonstrable facts and/or expert opinion.

6.4.2. Context

The context within which information occurs has a direct and important impact upon its interface with privacy law and policy. Individual data elements will, even when viewed in isolation, have a much higher likelihood of being characterized as being identifiable if they form part of a data set that is highly sensitive. So, for example, the "province" data field in *Gordon* was found to constitute identifiable information in part because the data set as a whole related to individuals who had suffered adverse (sometimes fatal) drug interactions. It seems unlikely that a similar finding would have been made had the data set related to recipients of commemorative postage stamps issued by Canada Post.

The context within which information occurs also becomes important when the data set at issue is of a small size. Using the "province" data field as an example once again, the possibility that an individual could be identified through the use of that information is amplified when the number of individuals across Canada represented in the data set is small. Obviously, if a data set contained information concerning only one resident of Alberta, the disclosure of the province data field could in some cases be tantamount to the release of that individual's name and address (i.e., if the larger data set concerned an attribute or condition that the individual was known by third parties to possess). Such concerns remain relevant even when the number of individuals represented in the data set increases; the point at which the size of the community of data subjects ceases to be relevant will vary in accordance with a number of factors that include (i) the sensitivity of the data and the (ii) amount and nature of other data elements being released from the same data set. In the latter case, the province of residence of one individual might still be personal information in a situation where one hundred other individuals represented in the data set resided in the same province, if the gender, age and ethnic origin of individuals represented in the data set had already been released. Only a careful assessment of the significance of individual data elements in the particular circumstance of each case can result in them being treated in an appropriate and privacy law compliant fashion.

6.4.3. Consultation

When in doubt - and sometimes even when not in doubt - consult! Given the uncertainties that can arise when attempting to characterize data elements as either personal or non-personal information or to properly deal with information that has been designated as being identifiable, federal officials would be well-advised to consult with other resources within their organization (or outside, if properly authorized) when confronted with such a task. In this regard, both Access to Information and Privacy (ATIP) personnel and legal counsel can be of great assistance because of their respective skills and expertise in matters relating to the application of the *Access to Information Act* and the *Privacy Act*. As the prevailing interpretation of the rules imposed by those Acts are subject to constant evolution due to ongoing inputs received from the courts, TBS and the OPCC, assistance from experts within your organization can help to ensure that program decisions reflect the current state of the law, government policy and privacy best practices. To the extent that technological solutions (such as "masking" of identifiable elements that are to be released) may help to resolve privacy-related issues that arise, consultation with organizational IT personnel would be warranted. Similarly, internal Communications experts can be of great assistance in crafting any required messages to stakeholders relating to an organization's dealings with geospatial information.

Valuable insights can also be obtained through dialogue with officials at the OPCC and TBS. The OPCC's views are of particular value, as that organization that will be called upon in the first instance to deal with any complaint regarding the characterization of data by a federal government institution. In appropriate circumstances, useful insights can also be acquired from colleagues at other organizations that have dealt with analogous privacy issues pertaining to geospatial data. Agencies such as Statistics Canada and federally supported organizations such as GeoConnections have a wealth of experience in dealings with the control of identifiable and de-identified information. However, the merits of information and advice received from external sources should be assessed and endorsed, whenever possible, by internal experts before being relied upon for program purposes.

6.4.4. Consistency

Each federal organization should make a concerted effort to ensure that it adopts a consistent approach to dealings with potentially identifiable geospatial information. To achieve this end, organizations should consider maintaining a centralized record of how data elements are characterized and treated in particular circumstances, with a view to replicating that treatment in future if identical or analogous conditions should exist. So, for example, if the "province of residence" data field is de-identified in one case where data relating to adverse drug reactions is to be released to third parties, the same treatment should be accorded to any directly similar dealings with that same data field in the future, subject to any directions or advice to the contrary received from the courts or privacy regulators.

6.4.5. Cumulative

Geospatial data elements that are not identifiable when considered individually may become identifiable when combined with other data elements. This cumulative impact will vary depending upon the circumstances of each case, and thus will require fresh analysis each time that the circumstances and data elements change. As a general rule of thumb, the likelihood that data elements within a data set will

combine to create a subset of identifiable data increases with each data element that is added to the subset. This is especially true if any of the data elements relate to a specific individual or to a specific location. So, for example, a data set containing a postal code, a related street map and address numbers would in most cases be assessed as containing no personal information. This assessment might very well change if a data element were to be added indicating that the geographic area described by the postal code and map contained one individual suffering from a rare form of cancer.

6.4.6. Caution

"When in doubt, don't" is an appropriate initial approach to the issue of whether individual elements of geospatial data should be collected, used or released to third parties. This is not intended to recommend or support a reflexive refusal to deal with such data in all cases. Rather, it acknowledges the fact that issues surrounding privacy are complex and that caution should be exercised in cases where doubt exists. Ideally, a release of data will only occur when the federal institution, operating within the time constraints imposed by federal privacy and access to information law and policy, has assessed that data and made an informed decision regarding its identifiability and susceptibility to being released.

6.4.7. Constraint

When disseminating either identifiable or de-identified information to third parties, be sure to consider the merits of restricting the data recipient's rights via contract. One of the frequently voiced concerns regarding the potential for geospatial data to become re-identified relates to the possibility that non-personal data elements from various sources will be compiled by a downstream party in a manner that was never anticipated by the releasing parties. The likelihood of this occurring can be reduced, if not eliminated, if the releasing parties restrict the right of recipients to release the data to other parties or to combine it with data elements already in the possession of the recipients.

Similar contractual approaches are also discussed in "*The Dissemination of Government Geographical Data in Canada: Guide to Best Practices, 2008, version 2*". Another means of reducing the likelihood that downstream parties can re-identify information is through the use of metadata. Metadata can provide descriptive information about a piece of data, for example:

- Who created the data? Who maintains it?
- What is the content of the data? What is its structure? What is the scale?
- Where is the geographic location? Where is it stored?
- When was the data collected? When was it published?
- Why was the data created?
- How was it produced? How can it be accessed? What data quality can you expect?

Metadata can prescribe downstream uses of geospatial data, including placing restrictions on other users taking steps that may re-identify the data.

7. Conclusion

At the request of Geoconnections and the Federal Government Geospatial Privacy Advisory Group, this *Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies* has been produced by CanadaPrivacy Services Inc. to examine the interface between privacy and geospatial information in the federal public sector in Canada. In particular, it has sought to:

- define key terms that are of relevance to the issue of privacy in a geospatial context in Canada;
- explore the meaning of geospatial information;
- provide a brief background concerning the development of geospatial information in Canada;
- assess the privacy impacts of geospatial information in Canada;
- examine the legal and policy environments within which dealings with geospatial data by federal government institutions take place;
- explore the meaning of "personal information" at law in Canada and assess whether the point(s) at which geospatial information becomes personal information can be accurately identified;
- furnish guidelines, including the *Seven "C's" of Geospatial Privacy*, for identifying and mitigating privacy-related risks and issues arising from the collection, use, retention, disclosure and disposition of personally identifiable geospatial information; and
- communicate the results of an inventory of geospatial data sets held by federal government institutions.

The Guide has identified a number of key privacy issues that federal officials should consider when dealing with geospatial data. These issues, and related mitigation recommendations, are encapsulated in section 6 of the Report. Taken together, they reveal a common theme: that privacy compliance, while sometimes complex, can nonetheless be attained if government institutions implement appropriate processes and assign suitable resources to their privacy compliance initiatives. This communal goal can be facilitated by the continuing role of Geoconnections and its federal government partners in producing guidance materials for the edification of members of the geomatics community. Privacy issues tend to evolve over time with changes to technology and/or to the relevant privacy rules (whether derived from statute, policy or court decision). Consequently, this Guide should be periodically reviewed and revised in order to maintain its currency and utility.

Questions regarding the Guide should be directed to the Manager, Communication & Policy Coordination at Natural Resources Canada, 615 Booth Street, 6th Floor, Room: 642X, Ottawa, Ontario, Canada, K1A 0E9

8. Appendix A – Bibliography

8.1. Publications

Abdel, Malik, Philip, et al. "The Perceived Impact of Location Privacy: A Web-Based Survey of Public Health Perspectives and Requirements in the UK and Canada", in *BMC Public Health*, 2008, vol. 8, p. 156.

Agriculture and Agri-food Canada. *National Land and Water Information Service: Documentation User Guide*.

AMEC Earth & Environmental. *Best Practices for Sharing Sensitive Environmental Geospatial Data, Version 1*, March 2010.

ANZLIC Spatial Information Council, *ANZLIC Best Practice Guideline, Spatial Information—Privacy Issues, Discussion Paper*, Version 2.0 (Final), 13 February 2004

ANZLIC Spatial Information Council, *ANZLIC Spatial Information Privacy Best Practice Guideline*, Version 2.0 (Final), 13 February 2004

ANZLIC Spatial Information Council, Spatial Information Industry Joint Steering Committee, *Discussion Paper: Respective Roles and Conduct of Relationships between the Public and Private Sectors in the Australian Spatial Information Industry*, Version 5.0, 2002

ANZLIC Spatial Information Council, *Discussion Paper: Access to Sensitive Spatial Data*, July 2004

ANZLIC Spatial Information Council, *Guidelines For Custodianship*, April 1998

Armstrong, Marc P., et al. "Geographic Information Technologies and Personal Privacy", in *Cartographica*, Volume 40, Issue 4, 2005.

Assistant Privacy Commissioner of Canada, *Getting Privacy Right in a World of "Mashups" and "Renonymizing"*, Remarks at the Geomatics Industry of Canada Annual Leaders Forum, Ottawa, Ontario, June 17, 2009.

Assistant Privacy Commissioner of Canada, *Privacy and the Changing World of Maps*, Remarks at the PIPA Conference 2009, Vancouver, British Columbia, October 15, 2009

Campbell, Lisa Madelon and Caron, Daniel. "The Unique Challenges to Privacy Rights Posed by the Internet and Other Emerging Technologies", *Internet Law Conference: The Second Wave: New Developments, Challenges and Strategies*, Toronto, March 27-28, 2008.

Bennett, Colin J. and Regan, Priscilla M. "What Happens When You Make a 911 Call?", in *Privacy and the Regulations of Cellular Technology in the United States and Canada*, 2002.

Beresford, Alastair R. "Privacy Issues in Geographic Information Technologies", in *Frontiers of Geographic Information Technology*, New York: Springer, 2006.

Devi, T.S. Gayathri, et al. "Public Access to Government Geographic Information in the Electronic Age", in *Data Driven: Database Design and Maintenance*, 2000.

El Emam, Khaled, et al. "Evaluating Predictors of Geographic Area Population Size Cutoffs to Manage Re-Identification Risk", *The Journal of The American Medical Informatics Association*, Volume 16, Issue 2, 2009.

GeoConnections. *The Dissemination of Government Geographic Data In Canada: Guide To Best Practices*, Version 2, 2008.

Government of the United States of America, Federal Committee on Statistical Methodology, Office of Information and Regulatory Affairs, Office of Management and Budget. *Statistical Policy Working Paper 22: Report on Statistical Disclosure Limitation Methodology*, December, 2005.

Info Source (http://www.infosource.gc.ca).

Information and Privacy Commissioner Ontario, *Geographic Information Systems*, 1997.

Jafarian, Jafar, et al. "Protecting Location Privacy through a Graph-Based Location Representation and a Robust Obfuscation Technique", in *ICISC 2008 (Lecture Notes in Computer Science)*, 2009.

Jain, Dharmesh. *A Discussion of Spatial Data Privacy Issues and Approaches to Build Privacy Protection in Geographic Information Systems*, 2002.

KPMG Consulting, *Geospatial Data Policy Study*, March 28, 2001.

Kwan, Mei-Po, *Protection of Geoprivacy and Accuracy of Spatial Information: How Effective are Geographical Masks?*, in *Cartographica*, 2004.

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

Morgan, L. Joe. *New Dimensions in Privacy: Spatial Privacy in the Geographic Information Age*,

Office of the Privacy Commissioner of Canada, *Briefing Note*, Workshop on Geospatial Information Technology, June 10, 2009.

- *Fact Sheet: Captured on Camera, Street-level Imaging Technology, the Internet, and You*.

- *Getting Privacy Right in a World of "Mashups" and "Renonymizing"*, Geomatics Industry of Canada Annual Leaders Forum, Ottawa, June 17, 2009.

- *Privacy and the Changing World of Maps*, PIPA Conference 2009, Vancouver, October 15, 2009.

Proposed Canadian Government Action Plan On Geospatial Data Policy, Canadian Council On Geomatics (CCOG) Annual Meeting Fredericton, New Brunswick 23 October 2001.

Statistics Canada, *Data Quality and Confidentiality Standards and Guideline*.

- *How Postal Codes Map to Geographic Areas*.
- *Postal Code Conversion File, Reference Guide*.

Treasury Board of Canada Secretariat, *Directive on Social Insurance Number*, 2008

- *Guidelines for Privacy Breaches*, 2007.
- *Standard on Geospatial Data*, 2009.

8.2. Case Law

Canada (Information Commissioner) v. Canadian Transportation Accident Investigation & Safety Board, 2006 CarswellNat 1277, 2006 FCA 157, 49 C.P.R. (4th) 7, 348 N.R. 263, 267 D.L.R. (4th) 451, [2007] 1 F.C.R. 203, 50 Admin. L.R. (4th) 43 (F.C.A.).

Canada (Information Commissioner) v. Royal Canadian Mounted Police Commissioner (2003), 47 Admin. L.R. (3d) 1, 24 C.P.R. (4th) 129, 224 D.L.R. (4th) 1, 301 N.R. 41, (sub nom. Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)) [2003] 1 S.C.R. 66, 239 F.T.R. 315 (note), 2003 CarswellNat 448, 2003 CarswellNat 449, 2003 SCC 8 (S.C.C.)

Dagg v. Canada (Minister of Finance) (1997), [1997] 2 S.C.R. 403, 46 Admin. L.R. (2d) 155, 132 F.T.R. 55 (note), 1997 CarswellNat 870, 1997 CarswellNat 869, 148 D.L.R. (4th) 385, 213 N.R. 161 (S.C.C.)
Gordon v. Canada (Minister of Health), 2008 CarswellNat 522, 2008 FC 258, 324 F.T.R. 94 (Eng.), 79 Admin. L.R. (4th) 258 (F.C.).

Gordon v. Canada (Minister of Health) (2008), 2008 FC 258.

Information Commissioner of Canada v. Canadian Transportation Accident Investigation & Safety Board (2007**),** 368 N.R. 396 (note).

H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General) (2006), [2006] 1 S.C.R. 441, 42 Admin. L.R. (4th) 1, 2006 SCC 13, 2006 CarswellNat 903, 2006 CarswellNat 904, 48 C.P.R. (4th) 161, 347 N.R. 1, 266 D.L.R. (4th) 675 (S.C.C.)

Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002] 2 S.C.R. 773, 2002 SCC 53.

Montana Band of Indians v. Canada (Minister of Indian Affairs & Northern Development), [1989] 1 F.C. 143.

R. v. Hutchings (1996), 1996 CarswellBC 2150, 39 C.R.R. (2d) 309 (B.C.C.A.), leave to appeal refused [1997] 2 S.C.R. x.

R. v. Plant [1993] 3 S.C.R. 281, 1993 CarswellAlta 194, 1993 Carswell Alta 566 (S.C.C.).

R. v. Tessling, (2004), 244 D.L.R. 541, 2004 CarswellOnt 4352 (S.C.C.).

Tridel Corp. v. Canada Mortgage & Housing Corp. (1996), 115 F.T.R. 185 (F.C.T.D.)

9. Appendix B – Geospatial Data Sets Inventory Report

Natural Resources Canada

Geospatial Data Sets Inventory Report

Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies

Draft Inventory Report

March 31, 2010

Document Change Control Table

Version	Date	Description	Author
Draft Geospatial Data Sets Inventory Report	February 23, 2010	Geospatial Data Sets Survey Results	CanadaPrivacy Services Inc.
Second Draft Geospatial Data Sets Inventory Report	March 17, 2010	Geospatial Data Sets Survey Report results reflecting comments from client	CanadaPrivacy Services Inc.
Final Inventory Report	March 31, 2010	Geospatial Data Sets Survey Report results reflecting comments from client	CanadaPrivacy Services Inc.

Table of Contents

Document Change Control Table 44
Table of Contents 45
Table of Figures 45
Executive Summary 47
1. Introduction 50
2. The Inventory Process 51
2.1. Phase Two: Inventory Tool Administration 51
3. Tabular and Textual Compilation of Inventory Results 51
3.1. Master Listing of Data Sets by Institution 51
3.2. Characterization of Information 52
3.3. Data Set Medium/Format and Volume 54
3.4. Accuracy of Record Groups 55
3.5. Source of Information 56
3.6. Authority for Data Collection 57
3.7. Purpose of Data Collection 57
3.8. Minimization and Alternatives to Collection 58
3.9. Use and Disclosure of Information 59
3.10. Data Set Database Management System 60
3.11. Data Set Security Features 60
3.12. Data Set Retention and Disposal Practices 61
3.13. Respondent Comments Not Captured Above 62
3.14. Data Source Statistical Wrap-up 63
4. Appendix A – Listing of all Participants 64

Table of Figures

Figure 4 - Highlights of Inventory Findings 50
Figure 5 - Table of Geospatial Information Sources by Government Institution 52
Figure 6 - Table of Characterization of Information 54
Figure 7 - Table of Data Source Formats and Size 55
Figure 8 - Accuracy of Records in Record Group 56
Figure 9 – Source of Information 56

Figure 10 - Authority for Information Collection..... 57
Figure 11 - Purpose of Information Collection 58
Figure 12 - Data Collection Minimization..... 59
Figure 13 - Use and Disclosure of Information 59
Figure 14 - Data Source Management System..... 60
Figure 15 - Data Source Security Features 61
Figure 16 - Retention and Disposal Practices..... 62
Figure 17 - Respondent's Additional Comments..... 63

Executive Summary

CanadaPrivacy Services Inc. ("CPSI") was engaged to develop an Inventory questionnaire with input from Geoconnections representatives. The questionnaire was completed on eight occasions via interviews conducted by CPSI with government officials associated with geographic data sources maintained by seven federal government institutions (one institution, Fisheries and Oceans Canada, completed surveys relating to two data sources). CPSI completed one additional questionnaire based upon information concerning a data source provided to it on an earlier date, for a total of nine completed surveys representing 702 Data Sets. This report provides a consolidation and interpretation of the survey responses relating to these nine federal data sources and their associated 702 Data Sets. It is noteworthy that only two institutions reported that the data sources under their control and custody contain personal information; the remaining 700 reported that the maintenance of their respective data sources does not involve the collection, use, storage, disclosure or disposal of any personal information. However, it is believed that three of those 700 Data Sets might contain identifiable information in certain limited circumstances.

Figure 1 below summarizes observations and the impact of those observations derived from the inventory of the aforementioned nine geospatial information sources:

No	Observation	Impact
1.	Two geospatial web portals (NLWIS and Mapster) collectively represent 695 Data Sets. Those Data Sets are designed to not contain any personal information.	For the overall inventory, there are 698 Data Sets that are designed to not contain any personal information: • Mapster (425) • NLWIS (270) • DMTI Spatial Inc (1) • Hydrographic charts (1) • Census Tract Profile (1) Total : 698 In addition, four other Data Sets were reviewed and of those, there are two Data Sets that could contain personal information if overlaid with other geospatial information (GeoPostPlus, National Geographic Database), and two that contain personal information. These numbers show that 99.7% of the Data Sets used for this inventory do not contain personal information.
2.	Given the lack of any centralized information registry for federal government institutions other	The fact that the identifiability of information elements associated with two of the 702 Data Sets (.3%) is

No	Observation	Impact
	than *Info Source* (which is generally not detailed enough to reference individual data sets), it is impossible to know precisely how many geospatial/geographic data sets are maintained by the government of Canada and, as a result, it is impossible to state categorically that the nine data sources examined during the course of this Inventory are representative of the government's overall geospatial data set holdings. Nonetheless, it is believed that the data sources identified during the course of this Inventory provide a reasonably representative sampling of the types of geospatially oriented personal information and other information that is currently in the custody and under the control of federal government institutions. Extensive efforts were made to involve more government institutions and to have officials associated with more data sets participate in the Inventory process; however, these efforts were ultimately unsuccessful as no additional participants could be secured. Data Sets that definitely contained personal information accounted for two of the 702 Data Sets examined during the course of the Inventory. Two of the Data Sets, meanwhile, contained information that might constitute personal information in certain limited circumstances.	unclear illustrates the difficulties that frequently arise when attempting to determine whether or not information is identifiable/personal. Consequently, guidance materials to assist federal government officials to properly characterize the identifiability of their data holdings are of key importance.
3.	Of the 702 datasets reviewed, 698 are made available to the public and four are not made available to the public. Of those that are publicly available (NLWIS, Census Tract Profile, Mapster, Navigational Charts and GeoPost Plus) none contain personal information. This has been accomplished through the pre-disclosure anonymization of any identifiable information contained in the subject Data Sets. However, none of the Data Sets possess any technological or legal/contractual features designed to completely prevent a downstream user from blending the anonymized data with other data to produce "renonymized" (i.e., re-identified) personal information.	Attempting to understand the circumstances in which non-personal geospatial information may be converted through combination with other data into personal information is core to this Inventory exercise. The Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies will consider the available means of controlling downstream use of anonymized data via technological or legal/contractual means.
4.	Only one of the Data Sets relies on data collected by a government institution directly from individuals (Census Tract Profile) and, in that case, the government institution aggregates that information prior to making it publicly available. The remaining Data Sets contain information obtained indirectly from provincial, municipal and private sector sources. This includes the two Data Sets that	Suggests that federal government geospatial systems containing personal information may frequently rely upon indirectly collected information, including personal information. This highlights the need for consideration of the *Privacy Act* requirement that institutions collect personal information directly from the individual concerned unless specific circumstances exist. It may also give rise to

No	Observation	Impact
	definitely contain personal information (2006 Prairie Agricultural Region and Land Owners Consultation Database).	concerns about the accuracy of the data collected.
5.	The oldest data in use in the Data Sets is from 1996 (14 years old). Most data is updated on a more routine basis or is used for a single operation where the currency of the data is deemed to be acceptable for that particular use.	Both the Canadian Standards Association's Model Code for the Protection of Personal Information, and the *Privacy Act* require that organizations take reasonable steps to ensure that the personal information is as accurate, up-to-date and complete as possible. The data collected during the inventory suggests that the data found in geospatial data sets is sufficiently current/accurate for its intended use.
6.	Of the two data sources that clearly maintain personal information, both could identify a program or statutory requirement for that personal information. Two of the data sources could identify statutory requirements to collect and use the data, while the remaining five data source could not identify a statutory basis for the collection and use of the data.	For those data sources that do not involve personal information, identifying a statutory requirement to collect data may not be very important. However, it is of prime importance when dealing with personal information that appears susceptible to renonymization.
7.	Two of the Data Sets' managers sought alternatives to the collection and use of personal information and of those two Sets, only one actually contains personal information. Four of the Data Sets' managers stated that they did go through an exercise to minimize the personal information that might be involved in their data.	It appears that Data Set managers are aware of privacy risks, as witnessed by the fact that they have taken steps to minimize the collection, use and retention of personal information. The majority of the Data Sets do not contain explicitly personal information.
8.	The Data Sets that are designed for internal use within a government institution restrict access to the data to only those employees who have a need to know the data. The Data Sets that are explicitly public are designed for open access and are not restricted. Others, such as the GeoPost Plus, are available to users on a limited, commercial basis.	The Data Sets containing personal information appear to have adequate controls in place to ensure that access to that information is restricted to those authorized individuals with an operational need-to-know.
9.	None of the data in the Data Sets reside in servers located outside of Canada or that are controlled by non-Canadian entities.	Indicates that there are no issues with respect to the USA PATRIOT Act with respect to the Data Sets.
10.	Two of the Data Sets have been the subject of Threat and Risk Assessments, two have been the subject of Privacy Impact Assessments, and the remaining 698 were not subject to any formal evaluation for security and/or privacy concerns. Neither of the two Data Sets that contain explicitly personal information (2006 Prairie Agricultural Region and Land Owners Consultation Database) have been the subject of a PIA.	Indicates that the majority (99.4%) of the Data Sets were not assessed for security or privacy risks. The fact that the two Data Sets that contain explicitly personal information have not been the subject of a PIA is of particular concern, as new federal systems containing personal information have, since 2002, been required by government policy (TBS' *Privacy Impact Assessment Policy*) to perform PIAs in most cases.

No	Observation	Impact
11.	One Data Set was determined to contain sensitive information, five contain information that is in the public domain, and the remaining three contain information that is either designated under the *Policy on Government Security* (Protected A) or is dealt with in a manner whereby it is not disseminated.	The *Policy on Government Security* and its associated *Operational Security Standard: Management of Information Technology Security* (MITS) require that government institutions identify and categorize information according to their sensitivity. There appears to be a lack of clarity by the Data Set managers with respect to the classification or designation of the information contained in the Data Sets., suggesting that privacy/security training may be of value to officials responsible for data holdings.
12.	Of the two Data Sets that contain explicitly personal information (2006 Prairie Agricultural Region and Land Owners Consultation Database), neither reported having a Personal Information Bank (PIB) registered in TBS' *Info Source*.	Suggests a significant degree (100%) of non-compliance with sub-section 10 (1) of the *Privacy Act*, *which* requires the head of the government institution to develop a PIB for personal information that has been, is, or is available for use for an administrative purpose or is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to the individual.
13.	Among the Data Sets, regardless of whether they contain personal information or not, only one has an information retention and disposition plan (2006 Prairie Agricultural Region). None of the information contained in that Data Set has ever been disposed of, despite the retention and disposition plan stating that the information should be retained for five years.	None of the Data Sets are managed in accordance with retention and disposition plans or authorities issued by the Librarian and Archivist of Canada, as required by the *Library and Archives of Canada Act*. More education is required to rectify this problem.
14.	One respondent noted that maintaining a geospatial data set that contains personal information is problematic without the appropriate rules, policies and procedures to protect that data. No other substantive comments relating to privacy matters were provided by the remaining eight Data Set respondents.	Reflects a high level of comfort with respect to the management of the Data Sets, but suggests a need for privacy/security-related training for managers of Data Sets, regardless of the perceived presence or absence of personal information.

Figure 4 - Highlights of Inventory Findings

10. Introduction

This Geospatial Data Set Inventory Report is intended to provide background information related to the nature, extent, sensitivity, location and format of federal government geospatial information holdings.

This, in turn, will (i) provide research results to be used as the development of the matrix of geospatial information, and (ii) facilitate the identification of the point at which geospatial information could be to be considered personal information as defined by the *Privacy Act* and/or the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

This report reflects a representative sampling of federal government Data Sets/data sources obtained through interviews with officials of several federal government institutions.

11. The Inventory Process

11.1. Phase Two: Inventory Tool Administration

The questionnaire was completed on eight occasions via interviews conducted by CPSI with government officials associated with data sets maintained by seven federal government institutions (one institution, Fisheries and Oceans Canada, completed surveys relating to two sets of geospatial information). CPSI completed one additional questionnaire based upon information concerning a data set provided to it on an earlier date, for a total of nine completed surveys representing 702 Data Sets. This report provides a consolidation and interpretation of the survey responses relating to these nine federal data sources and their associated 702 Data Sets. It is noteworthy that only two institutions reported that the data sources under their control and custody contain personal information; the remaining 700 reported that the maintenance of their respective data sources does not involve the collection, use, storage, disclosure or disposal of any personal information. However, it is believed that three of those 700 Data Sets might contain identifiable information in certain limited circumstances.

12. Tabular and Textual Compilation of Inventory Results

12.1. Master Listing of Data Sets by Institution

The nine geospatial information data sources are outlined in the table in Figure 5 below. For each data source, the responsible government institution is indicated in the column titled Inventory Interview Identification. Those data sources that reported the existence of personal information as part of the associated information holdings are indicated with in green, those that clearly did not have personal information are in red, and those thay might possibly have personal information, especially if their data are blended with other data, are in yellow. For each data source, the column on the far right indicates if the data source is available to the public or not.

Data Source #	Government Institution	Inventory Interview ID	# of Data Sets	Data Source Name	Personal Information No/Yes/Possibly	Publicly Available
1.	**Agricultre and Agri-food Canada**	20091208AAFC	1	2006 Prairie Agricultural Region		No
2.	**Canada Post**	20091214CPC	1	GeoPost Plus		Yes

Data Source #	Government Institution	Inventory Interview ID	# of Data Sets	Data Source Name	Personal Information No/Yes/Possibly	Publicly Available
	Corporation					
3.	**Public Safety Canada**	20100105PSC	1	DMTI Spatial Inc.		No
4.	**Elections Canada**	20100112EC	1	National Geographic Database		No
5.	**Parks Canada**	20100118PC	1	Land Owner Consultation Database		No
6.	**Fisheries and Oceans (Canadian Hydrographic Services)**	20100118DFO	1	Electronic Navigational Chart Index		Yes
7.	**Fisheries and Oceans**	20100121DFO	425	Mapster		Yes
8.	**Statistics Canada**	20100204SC	1	Census Tract Profile		Yes
9.	**Agriculture and Agri—Food Canada**	20100118AAFC	270	National Land and Water Information System		Yes
	Total Number of Data Sets		702			

Figure 5 - Table of Geospatial Information Sources by Government Institution

12.2. Characterization of Information

Data Set Number	Data Set /Source of Information	Personal Information	Class of Individuals Concerned
1.	2006 Prairie Agricultural Region	One Data Set containing Prairie crop insurance information that includes cadastre parcel location information on producers and their client number, if a claim was made and if insurance was paid out, but not the amount. AAFC does not receive names, telephone number or addresses but works with the provincial insurance plans, on the basis of the producer's client number, to verify if the claim is valid.	Agricultural producers in the Crop Insurance program who have subscribed to production insurance.

Data Set Number	Data Set /Source of Information	Personal Information	Class of Individuals Concerned
2.	GeoPost Plus	One Data Set of Postal codes by mail route.	Property owners within the geographic area of interest.
3.	DMTI Spatial Inc.	One Data Set that as used by Public Safety Canada, does not use personal information. Data is used by Public Safety to manage emergencies, such as floods.	N/A
4.	National Geographic Database	One Data Set that uses address ranges and institution does not consider the ranges to be personal information on their own.	N/A
5.	Land Owner Consultation Database	One Data Set that contains landowner name, location information and contact information.	Land owners, both private and commercial, whose properties intersect with park land.
6.	Electronic Navigational Chart Index	No personal information is contained in the one Data Set. System provides electronic nagivation charts. It is mandatory for mariners in Canada's waters to have paper or electronic navigation charts on board.	N/A
7.	Mapster	Mapster is not technically a Data Set, but rather a collection of 425 Data Sets arranged in a manner that enables visualization and analysis of multiple geospatial data elements. No personal information is contained in the system. Mapster is an Internet-based GIS application that provides access to fish and fish habitat related information for a widely dispersed and diverse group of users.	N/A
8.	Census Tract Profile	One Data Set that contains no personal information. This is a one of many products published by Statistics Canada that provide aggregate-level data on characteristics of the Canadian population. These products are derived, in part, from identifiable microdata (house-hold level) that is collected during either the census or specific surveys; however, the microdata are not presented in the	N/A

Data Set Number	Data Set /Source of Information	Personal Information	Class of Individuals Concerned
		product.	
9.	National Land and Water Information System	NLWIS is not technically a Data Set, but rather a collection of 270 Data Sets arranged in a manner that enables visualization and analysis of multiple geospatial data elements. System is not designed to contain personal information; however, it does enable users to view geographic information, such a latitude and longditude of specific quarter sections of farm land as well as information on soil classification, climate, topography, imagery, land use (agricultural), and water.	N/A

Figure 6 - Table of Characterization of Information

12.3. Data Set Medium / Format and Volume

Data Source #	Data Source Name	Data Source Format	Volume
1.	2006 Prairie Agricultural Region	High-resolutuion satellite imagery polygonal Cadastre parcels in electronic format	unknown
2.	GeoPost Plus	Electronic information	unknown
3.	DMTI Spatial Inc.	Electronic information	25 gigabytes
4.	National Geographic Database	Vector information available in Shape, GML and MapInfo formats by province for the whole country	0ver 1 million road arcs
5.	Land Owner Consultation Database	Electronic information in a GIS	400 megabytes
6.	Electronic Navigational Chart Index	Electronic chart reference system using chart names	Each chart is around 5 megabytes
7.	Mapster	Electronically manipulated geographic series of data sets (425)	500 gigabytes (estimated)

Data Source #	Data Source Name	Data Source Format	Volume
		using the Open GIS Consortium Web Map Service specification	
8.	Census Tract Profile	Internet-based application	5,000 census tracts
9.	National Land and Water Information System	Internet-based application using 270 data sets.	unknown

Figure 7 - Table of Data Source Formats and Size

12.4. Accuracy of Record Groups

Data Source #	Data Set/Source of Information	Date Span	Accuracy Comments
1.	2006 Prairie Agricultural Region	Satellite Imagery data circa 2003-2006, Crop Insurance data circa 2005-2006	Accurate to 2006
2.	GeoPost Plus	Based on last census (2006)	Based on last census (2006)
3.	DMTI Spatial Inc.	Quarterly updates	Quarterly updates
4.	National Geographic Database	Oldest sources are 1996 but carry out on-going updates	Oldest sources are 1996 but carry out on-going updates
5.	Land Owner Consultation Database	Landownership from and to dates, as land ownership is in constant flux	
6.	Electronic Navigational Chart Index	Data is current and Canadian Hydrographic Services (CHS) has 2 months to make new information publicly available	All charts have dates on them
7.	Mapster	Data does not change very fast, some are updated 2-4 times a years, but not most of them	
8.	Census Tract Profile	Current to last census (2006) and will be updated	

Data Source #	Data Set/Source of Information	Date Span	Accuracy Comments
		in 2011	
9.	National Land and Water Information System	Orthorectified images are dated May 12, 2001	

Figure 8 - Accuracy of Records in Record Group

12.5. Source of Information

Data Source #	Data Set/Source of Information	Source of Information
1.	2006 Prairie Agricultural Region	Provincial crop insurance program provide client number and claim information that AAFC overlays with GIS information and satellite Imagery from commercial vendor
2.	GeoPost Plus	Census data from Stats Canada and imagery data from Pitney Bowes
3.	DMTI Spatial Inc.	DMTI Spatial
4.	National Geographic Database	Census information from Statistics Canada, municipal and provincial information from those sources
5.	Land Owner Consultation Database	Provincial and municipal land owner records
6.	Electronic Navigational Chart Index	DFO and Coast Guard hydrographic surveys, independent contractor's surveys, provincial surveys and sometimes dredgers and other surveyors
7.	Mapster	DFO, Pacific Region, Habitat and Enhancement, the Province of British Columbia, Canada Centre for Remote Sensing, Demis and GIS Innovations
8.	Census Tract Profile	Direct collection and indirect collection from the individuals concerned during the census.
9.	National Land and Water Information System	Some datasets from rural ,municipalities, provincial governments and federal government sources.

Figure 9 – Source of Information

12.6. Authority for Data Collection

Data Source #	Data Set/Source of Information	Authority Cited
1.	2006 Prairie Agricultural Region	AAFC program requirements
2.	GeoPost Plus	No authority cited
3.	DMTI Spatial Inc.	Program requirements
4.	National Geographic Database	No authority cited
5.	Land Owner Consultation Database	Species At Risk Act
6.	Electronic Navigational Chart Index	Shipping navigation
7.	Mapster	No authority cited
8.	Census Tract Profile	Statistics Canada Act, British North America Act
9.	National Land and Water Information System	Major Crown Project - No authority cited

Figure 10 - Authority for Information Collection

12.7. Purpose of Data Collection

Data Source #	Data Set/Source of Information	Primary Purpose	Secondary Purpose
1.	2006 Prairie Agricultural Region	Crop Insurance payment and verification purposes	No secondary purposes
2.	GeoPost Plus	Postal codes are used primarily for directing and delivering mail.	Enables mailers (usually commercial entities) to have Canada Post assist them to target postal codes for mass mailing marketing
3.	DMTI Spatial Inc.	Public Safety produces geospatial products for government officials, or situational awareness products for emergency response, including flood information, forest fire information, tsunamis, etc.	No secondary purposes
4.	National Geographic Database	To develop and maintain a national road network file serving the needs of both Statistics Canada and Elections Canada.	No secondary purposes
5.	Land Owner Consultation Database	To enable Parks Canada to consult with land owners who own land affected by species at risk. Currently not carrying out these duties as they feel they are	No secondary purposes

Data Source #	Data Set/Source of Information	Primary Purpose	Secondary Purpose
		the responsibility of Environment Canada.	
6.	Electronic Navigational Chart Index	Navigational aids to shipping and mariners	No secondary purposes
7.	Mapster	Enables anyone to view different spatial datasets and retrieve database information including summary reports.	No secondary purposes
8.	Census Tract Profile	To publish aggregate census data on characteristics of the Canadian population and to use to analyze other data and data products	No secondary purposes
9.	National Land and Water Information System	To provide a recognized source of information, analysis and interpretation of land, soil, water, climatic and biodiversity data to assist land-use managers in their agri-environmental planning.	No secondary purposes

Figure 11 - Purpose of Information Collection

12.8. Minimization and Alternatives to Collection

Data Source #	Data Set/Source of Information	Were Alternatives to Collecting Personal Information Explored?	Was Personal Information Collection Minimized?
1.	2006 Prairie Agricultural Region	No	Yes
2.	GeoPost Plus	No comment	No comment
3.	DMTI Spatial Inc.	N/A	N/A
4.	National Geographic Database	No	Yes
5.	Land Owner Consultation Database	Yes	Yes, only collect what is essential
6.	Electronic Navigational Chart Index	N/A	N/A
7.	Mapster	N/A	N/A
8.	Census Tract Profile	Yes	Yes, Census questions are set by Cabinet
9.	National Land and Water Information System	N/A	N/A

Figure 12 - Data Collection Minimization

12.9. Use and Disclosure of Information

Data Source #	Data Set/Source of Information	Personal Information Used By	Personal Information Disseminated To
1.	2006 Prairie Agricultural Region	Only by AAFC employees with a need to know	Information may be shared with provincial agricultural programs
2.	GeoPost Plus	Canada Post and clients of Canada Post	Non-personal information is disseminated to anyone wanting to do mass mailings by postal code.
3.	DMTI Spatial Inc.	Only PS employees with a need to know	No disclosure of personal information
4.	National Geographic Database	No personal information but data is used by Elections Canada and Statistics Canada	Public disclosure of non-identifiable information
5.	Land Owner Consultation Database	Four employees of Parks Canada	No disclosure of personal information
6.	Electronic Navigational Chart Index	No personal information but data is used by Canadian Hydrographic Service, some confidential charts are available to National Defense	Use of charts for navigation in Canadian waters is mandatory, but no personal information is disseminated.
7.	Mapster	No personal information but data is used by Fisheries and Oceans, British Columbia government	Geospatial data is available to the public – no personal information is disseminated
8.	Census Tract Profile	Very strict rules applied to use of personal information from Census or other surveys. Some staff have access to microdata, but most use aggregated data.	Aggregate data are available to the public through Statistics Canada website.
9.	National Land and Water Information System	No personal information is used within AAFC.	Geospatial information is made publicly available.

Figure 13 - Use and Disclosure of Information

12.10. Data Set Database Management System

Data Source #	Data Set/Source of Information	Management System	Location
1.	2006 Prairie Agricultural Region	Satellite imagery and Polygonal Cadastre parcels	AAFC secured geospatial archive
2.	GeoPost Plus	Geopost Plus system and MapInfo from Pitney Bowes – they use a software product called Target Pro	Data reside in a database in Montreal
3.	DMTI Spatial Inc.	DMTI Spatial product called CanMap Street Files	Servers in Ottawa
4.	National Geographic Database	National Geographic Database	Elections Canada
5.	Land Owner Consultation Database	Parks Canada GIS system	Calgary and Winnipeg
6.	Electronic Navigational Chart Index	CHS Geo Portal	DFO and CHS servers in Ottawa
7.	Mapster	GIS application called Mapster	Online at DFO Pacific Regional Office website
8.	Census Tract Profile	StatsCan data analysis system	Tunney's Pasture, Ottawa
9.	National Land and Water Information System	NLWIS at AAFC	Online

Figure 14 - Data Source Management System

12.11. Data Set Security Features

Data Source #	Data Set/Source of Information	Security Classification	Statement of Sensitivity Done?	Threat & Risk Assessment Done?
1.	2006 Prairie Agricultural Region	Protected A	Yes	Yes
2.	GeoPost Plus	N/A – data are public	Unknown	Unknown
3.	DMTI Spatial Inc.	Unknown – but never disseminated to public	Unknown	Unknown

Data Source #	Data Set/Source of Information	Security Classification	Statement of Sensitivity Done?	Threat & Risk Assessment Done?
4.	National Geographic Database	Not protected or classified	N/A	N/A
5.	Land Owner Consultation Database	Sensitive	Unknown	Unknown
6.	Electronic Navigational Chart Index	Public	No	No
7.	Mapster	Public	Yes	Yes
8.	Census Tract Profile	Public	No, but did a PIA	No, but did a PIA
9.	National Land and Water Information System	Public	No, but did a PIA	No, but did a PIA

Figure 15 - Data Source Security Features

12.12. Data Set Retention and Disposal Practices

Data Source #	Data Set/Source of Information	Personal Information Bank (reported)	Personal Information Bank (actual)	Retention and Disposal Practices	Method of Destruction
1.	2006 Prairie Agricultural Region	None	No PIB identified	Retained for 5 years, but nothing actually destroyed	N/A
2.	GeoPost Plus	None	No PIB required	New data overwrites older data	N/A
3.	DMTI Spatial Inc.	None	No PIB identified	New data overwrites older data	N/A
4.	National Geographic Database	Yes	No specific PIB identified, but possibly the National Register of Electors (CEO PPU 037) applies	Respondent indicated that data are not destroyed; however, if CEO PPU 037 applies, data are destroyed after two years.	N/A
5.	Land Owner Consultation Database	Unknown	No PIB identified	Unknown	Unknown

Data Source #	Data Set/Source of Information	Personal Information Bank (reported)	Personal Information Bank (actual)	Retention and Disposal Practices	Method of Destruction
6.	Electronic Navigational Chart Index	Unknown	Class of Records Number DFO SCI 615 was identified as applying to this data	New data overwrites older data; older data is maintained for legal purposes, never deleted	N/A
7.	Mapster	Unknown	No PIB or Classs of Record was identified	New data overwrites older data; older data is maintained for legal purposes, never deleted	N/A
8.	Census Tract Profile	Yes	STC PPU 005, Census of Population Questionnaire	Archived in perpetuity	N/A
9.	National Land and Water Information System	Unknown	AAFC 3200, environmental Monitoring Institutional Class of Records	Unknown	Unknown

Figure 16 - Retention and Disposal Practices

12.13. Respondent Comments Not Captured Above

Data Source #	Data Set/Source of Information	Comments/Questions
1.	2006 Prairie Agricultural Region	All data are collected and used only as needed
2.	GeoPost Plus	All the data are location-based by postal code along with probabilities related to the characteristics of the residents within that geographic area
3.	DMTI Spatial Inc.	No comments
4.	National Geographic Database	No comments
5.	Land Owner Consultation Database	Holidng this data is problematic as they do not have any

Data Source #	Data Set/Source of Information	Comments/Questions
		rules, policies or guidance on how to manage it, making a mistake with it woud be a problem, would prefer a secure system with procedures
6.	Electronic Navigational Chart Index	No comments
7.	Mapster	Not using personal information makes this system easier to manage
8.	Census Tract Profile	Confident that they apply appropriate protection and policies and procedures
9.	National Land and Water Information System	No comments

Figure 17 - Respondent's Additional Comments

12.14. Data Source Statistical Wrap-up

Number of Data Sources	9
Number of Data Sets	702
Location of Personal Information	All in Canada: Montreal, National Capital Region, Winnipeg Calgary
Categories of individuals associated with Data Sets that contain or may contain personal information:	• Agricultural producers in the Prairies (Agriculture and Agri-food Canada) • Land owners near Crown lands (Parks Canada) • Addressees in Canada (Canada Post) • Electors in Canada (Elections Canada) • Agricultural land owners, rural land owners (Agriculture and Agri-food Canada)
Data Sets Format	All (702) Data Sets are in electronic information systems, either on-line or network based geographic systems
Authority to collect personal information	Of the 2 Data Sets that definitely contain personal information, both can cite a statutory basis for the collection
Oldest Data Sets	1996
Number of Data Sets sharing information	702
Data Sets that collect personal information	1

directly from the individual concerned	
Data Sets that collect personal information indirectly	2
Number of Data Sets where data minimization excersise occurred	3
Security Description of Data Source	Public – Protected A
Use of personal information	Crop Insurance payment processing, *Species Act Risk Act* management and census
Data Sets with documented Personal Information Banks	2
Retention and Disposal Plans	No Data Sets had an official record retention and disposition plan
Disposal Practices	None of the data involved in the Data Sets is disposed of

Figure 19 - Data Set Statistical Wrap-up

13. Appendix A – Listing of all Participants

Item #	Government Institution	Data Set/Geospatial Information Source Name	Inventory Interview ID
1.	**Agricultre and Agri-food Canada**	2006 Prairie Agricultural Region	20091208AAFC
2.	**Canada Post Corporation**	GeoPost Plus	20091214CPC
3.	**Public Safety Canada**	DMTI Spatial Inc.	20100105PSC
4.	**Elections Canada**	National Geography Database	20100112EC
5.	**Parks Canada**	Land Owner Consultation Database	20100118PC
6.	**Fisheries and Oceans (Canadian Hydrographic Services)**	Electronic Navigational Chart Index	20100118DFO
7.	**Fisheries and Oceans**	Mapster	20100121DFO
8.	**Statistics Canada**	Census Tract Profile	20100204SC
9.	**Agriculture and Agri—Food Canada**	National Land and Water Information System	20100118AAFC