GEOGRAPHICAL INFORMATION AS 'PERSONAL INFORMATION'

TERESA SCASSA*

A Introduction

Maps have long been used to represent and display a wide variety of information. Placing information in a geographic context can give us new insights about social, political, environmental, demographic and other phenomena. Governments and businesses find value in placing information in a geographic context, and contemporary technology has greatly facilitated the combining and analysing of disparate sets of data. Web 2.0 and its associated tools and applications have also revolutionised the display and dissemination of such information by putting sophisticated tools in the hands of all manner of computer users. The democratisation of much government data has meant that there is a rich and ever-increasing supply of information that may be represented in geographical terms. Information about every conceivable phenomenon from diseases to crime incidents can now be placed in a geographic context by government actors, private sector companies or individuals—and frequently by all three.[1] The wide variety of data and the diversity of the publishers of data create significant challenges for data protection.

Data protection laws typically govern the collection, use and disclosure of personal information. The focus of this paper is on the threshold question for the application of data protection laws: when does information placed in a geographical context become personal information? Understanding this threshold question is important because of the way in which geographic information systems develop. In many cases, the starting point for an application is anonymised or de-identified data. Yet geographic information is often a key element in identifying or re-identifying individual data subjects. For those who make data available and

* Canada Research Chair in Information Law, University of Ottawa, Faculty of Law, Common Law Section. I gratefully acknowledge the support of the GEOIDE Network and the Canada Research Chairs program. Thanks also to the research assistance of Kelly Harris, Emilia de Somma, and Carmina Chan, and to Charles Sanders for his comments on an earlier version.

[1] In addition to mapping data onto geographic co-ordinates, a rich variety of location data is generated by a wide range of tools and devices. These include surveillance cameras, global positioning systems (GPS), cell phones, and Radio Frequency Identification (RFID)-embedded access cards. Location data is also generated when individuals use their credit cards in commerce, operate automated bank machines, or perform any one of a wide range of technology-enhanced activities.

those who develop applications that make use of it, the difficulty becomes anticipating when their collection, use or disclosure of data involves personal information. For those overseeing data protection regimes, the challenge is to protect personal information without unduly inhibiting either innovative data applications or the drive towards greater access to information in the public interest.

This paper explores issues that arise where previously anonymised or relatively anonymous information is placed in a geographic context. The question is when such information is 'personal information' such that it will attract the application of data protection norms. The question is of interest to those who release de-identified data sets for research or other purposes or under access to information laws. It is also relevant to those who develop data resources, including information maps, in the private sector. Although the paper focuses on Canadian data protection legislation, such legislation is based upon the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[2] which form the backbone of many data protection statutes worldwide. The paper begins with a brief overview geographic information systems and is followed by a discussion of the definition of personal information under data protection laws, and the challenges it presents.

B Geographical Information Systems

A geographical information system (GIS[3]) is a process or program that compiles, sorts and analyses geographical aspects of data. The recent rapid growth of GIS and the fascination with the unique ways in which information can be represented on maps means that government entities are often quick to embrace GIS as a way to make information publicly available in a readily accessible format. Thus, police forces may generate detailed maps, accessible for online viewing, that represent the nature and occurrence of crimes within their precincts.[4] Disease control authorities may post maps showing incidences and outbreaks of disease.[5] Geographical information traditionally recorded by governments (such as that in land registries,

[2] (Directorate for Science, Technology and Industry) <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html> accessed 30 December 2010 (OECD Guidelines). It defines personal data as 'any information relating to an identified or identifiable individual (data subject)': art 1(b).

[3] This abbreviation stands for 'geographical information systems' as well, depending on the context.

[4] The provision of crime information to the public in map form is increasingly commonplace. See, eg, the Ottawa Police Service, 'Ottawa Crime Statistics' <http://www.ottawapolice.ca/en/crimefiles/CrimeMaps_Reports/crimestats.aspx> accessed 1 January 2011.

[5] The Centre for Disease Control in the United States offers health information in map form for a wide range of diseases. For the map of incidences of West Nile Virus across the USA in 2008, see: <http://www.cdc.gov/ncidod/dvbid/westnile/Mapsincidence/surv&control08IncidMaps.htm> accessed 1 January 2011.

infrastructure maps and so on) may also now be published in much more widely accessible and digitised formats.[6]

It is not just governments that see the attraction and potential of GIS. Private sector companies have embraced GIS for their capacity to permit the combination of a wide variety of personal information with geographic location information to develop complex location-based views of target markets for their products. Information mapping by companies large and small (and by individuals as well) has been greatly facilitated by Google Maps. Google offers simple, easy to use, searchable, world-wide maps, in a format that enables and even encourages the development of mashups (new services created from a combination of sources) that plot other data onto its maps.[7] Commercial applications have emerged that combine diverse kinds of information with location information.[8] Google's Street View,[9] which combines video images with maps to create detailed and interactive views of geographic locations of all kinds, has been incorporated into other applications, such as online house-hunting tools.

The data that are combined with mapping applications may come from a variety of sources. Some data are provided to the public as part of an open government initiative. Other data are sought using access to information requests, or are culled from public records.[10] Non-governmental sources of data are virtually limitless, and can include real estate listings,[11] local business information, and the vast stores of information collected by private sector companies about their customers. There are also a growing number of opportunities for individuals to contribute to data mash-ups—applications that combine data, including geographic data, from a variety of sources. Many of these mash-ups invite users to

[6] See, eg, Information Services Corporation of Saskatchewan <http://www.isc.ca> accessed 1 January 2011; British Columbia Land Title & Survey, Online Cadastre < http://www.ltsa.ca/surveyor-general/online-cadastre> accessed 3 January 2011.

[7] See C C Miller, 'A Beast in the Field: The Google Maps Mashup as GIS/2' (2006) 41 Cartographica 187.

[8] See, eg, Yahoo! Real Estate <http://realestate.yahoo.com/neighborhoods> accessed 3 January 2011, which provides a broad range of information about neighbourhoods across the United States, including demographic information, information about schools and about crime. At the United Kingdom site <http://www.upmystreet.com> accessed 1 January 2011, searches based on postal codes will provide a wide spectrum of information about neighbourhoods across the UK. The information includes data about crime, schools, taxes, services, facilities, businesses, and the housing market.

[9] <http://maps.google.ca/help/maps/streetview/> accessed 24 November 2010.

[10] Some examples include: maps indicating locations in San Francisco with 100 or more parking ticket citations <http://www.sfgate.com/maps/parkingtickets/> accessed 24 November 2010 and a site that maps the US roads with the most fatal accidents <http://www.saferoadmaps.org> accessed 24 November 2010. Many of the maps at Toronto Star's Map of the Week use information gleaned from access to information requests: <http://thestar.blogs.com/maps/> accessed 24 November 2010.

[11] Zoocasa, a real estate website (<http://www.zoocasa.com/en/> accessed 3 January 2011), has recently been sued for its practice of scraping data from real estate listings to use in its site: Gary Marr, 'Century 21 Canada does battle with Rogers' *Financial Post* (Toronto, 7 September 2009) <http://www.financialpost.com/story.html?id=1969611> accessed 1 January 2011.

contribute information not typically associated with or normally captured by commercial applications, including information about private geographical spaces,[12] subjective views and opinions,[13] information about events or incidents,[14] photographs,[15] and a wide range of other information. Individuals now also have easy access to the tools that would allow them to create their own mash-ups—and this they are doing in large numbers.[16]

The result is a continuing evolution of GIS in a manner that sees its spread and use in a growing range of sectors and for an ever-increasing variety of purposes. The evolution also sees a decentralisation of the consumption, use and creation of GI based systems, tools and applications.[17] The continual evolution of the technology must be kept in mind in considering legal norms, as the changing nature of the data that is collected and the manner in which it is used may have important legal consequences.[18]

C Geographic Information and Data Protection

While information placed in geographic context has implications both for privacy rights[19] and for data protection, the primary focus in this paper will be on data protection. Data protection regimes fall under the general umbrella of 'privacy law', but rather than having as their primary objective the protection of a right to

[12] Eg Carpool Connect <http://www.programmableweb.com/mashup/carpool-connect> accessed 24 November 2010, helps set up carpools based on individuals' work and home addresses.

[13] Many restaurant review sites will locate restaurants reviewed by members of the public on maps.

[14] See, eg, the crowdsourcing map site Ushahidi, which allows users to contribute crisis information that can be visualised on a map: <http://www.ushahidi.com> accessed 3 January 2011. The news network Al Jazeera has created a crowd-sourced map titled 'War on Gaza', which invites users to contribute information, photographs and opinions on events in Gaza: <http://labs.aljazeera.net/warongaza/> accessed 3 January 2011.

[15] Many websites invite users to contribute photographs. For example, Panoramio allows users to contribute their own photographs of landmarks and other public spaces: <http://www.panoramio.com/> accessed 24 November 2010. The Northwest Dive News is an example of an online magazine that allows readers to contribute photographs: <http://divenewsnetwork.com/nwdive/?q=reader_photos> accessed 24 November 2010. See also BBC News <http://news.bbc.co.uk/2/hi/in_pictures/4779823.stm> accessed 24 November 2010. Spotted, an online site featuring photographs from events in Augusta, Georgia, invites users to contribute photographs: <http://spotted.augusta.com/> accessed 24 November 2010.

[16] Programmable Web keeps a very extensive list of mashups created using freely available online tools and data: <http://www.programmableweb.com/mashups> accesed 24 November 2010.

[17] Miller (n 7) 191–94.

[18] *R v Mahmood*, 2008 CanLII 51774 (Supreme Court of Ontario) set aside older case law on the reasonable expectation of privacy in relation to utility and other records precisely because of changes in how such data is collected, used and reported, and because of changing norms around data protection.

[19] For a recent article on privacy rights in relation to information in a geographic context see: Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy', (2009) 7(2) Canadian Journal of Law and Technology 1.

privacy (which often defines the limits of the state's permitted intrusion into the lives of individuals), they seek to balance the interests of either the state or the private sector in the collection, use and disclosure of personal information with the right of individuals to exercise control over their personal information.

1 Data Protection Challenges in GIS

The users and disseminators of information in a geographic context may be public or private actors, and this will affect any data protection analysis. The technologies are also in a state of constant evolution. While in some cases the privacy implications of a given application will be immediately obvious, in others they will be unclear. This makes a data protection analysis of this technology complex.

Privacy by design is touted as the ideal in the development of new applications and technologies.[20] However, privacy issues may not be taken into account in the design of some GIS as they may simply not be anticipated. This may be the case, for example, where two or more sets of data, none of which individually would identify particular individuals are combined. The combination of data sets may lead to the identification of individuals in ways which were not anticipated. Further, the data disclosed in one application may only lead to the identification of specific individuals when it is matched with other data from other sources. As technology advances, and as more and more data becomes available to enlarge existing compilations, the identification of individuals in these data products will occur almost from one moment to the next. As a result, information that is collected for one purpose but that is later combined in a GIS, may change its character significantly, and may have privacy implications within the GIS that it did not have on its own.[21]

Privacy by design is also easier for governments or large-scale enterprises with adequate resources and expertise to achieve. Web 2.0 and the Google Maps API,[22] for example, place the ability to create information maps in the hands of any reasonably computer literate individual. National governments are also committing to the free public dissemination of major sets of data, with a view to encouraging the development of innovative data-based products and services.[23]

[20] Eg Anne Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (Office of the Information and Privacy Commissioner of Ontario (Ontario OIPC)) <http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf> accessed 24 November 2010.

[21] This is because the added element of geographical location may provide the key needed to re-identify one or more individuals whose data is included in the set.

[22] API stands for Application Program Interface. The Google Maps API provides a relatively user-friendly means by which individuals can integrate Google Maps into their own web sites and can plot other information onto Google Maps. See 'What is the Google Maps API' <http://code.google.com/apis/maps/> accessed 24 November 2010.

[23] Consider, for example, the portals created in Canada and elsewhere for free access to collections of government geospatial data. In Canada, see Geobase <http://www.geobase.ca/> accessed 24

These developments mean that the creation and use of GIS is no longer limited to governments or corporations, and may frequently involve many players with little awareness of or interest in privacy issues and few resources to aid in anticipating or addressing them.

Compilations of data that are premised on the identification of specific individuals and their personal characteristics are relatively easy to address under a data protection regime that is designed to set the boundaries for this type of collection, use and disclosure. Compilations of data with other objectives but that may incidentally lead to the identification of particular individuals and the disclosure of personal information about them present a more difficult challenge for the balancing process. This has been aptly demonstrated by the launch of Google Street View. The filming of streetscapes to created interactive visual maps of cities around the world has, by capturing people on or near streets, car licence plates and other images, incidentally resulted in the collection, use and disclosure of information about identifiable individuals. Data protection in this context has focused more on managing the incidents than on implementing a consent-based framework for the collection, use and disclosure of personal information in the filming of streetscapes.[24]

2 Statutory definitions of personal information

Canadian data protection legislation governs two broad categories: the collection, use and disclosure of information in the public sector; and the same activity in the

November 2010 (providing geospatial data from all levels of government), and GeoGratis <http://geogratis.cgdi.gc.ca/> accessed 24 November 2010 (providing free geospatial data from the Earth Sciences Sector of Natural Resources Canada). In the United States, see the resources made available through the National Spatial Data Infrastructure <http://www.fgdc.gov/nsdi/nsdi.html> accessed 24 November 2010. For a clearinghouse of international governmental geospatial data initiatives, see Global Spatial Data Infrastructure Association <http://www.gsdi.org/SDIILinks> accessed 24 November 2010. Outside the context of spatial data infrastructures, there are numerous governmental initiatives to 'free' data. One that has received a fair amount of attention recently is the announcement by President Obama of the Open Government Initiative in the United States: <http://www.whitehouse.gov/open> accessed 24 November 2010. The US government data clearinghouse can be found at <http://www.data.gov/> accessed 24 November 2010. In the UK, the government has offered a prize for the most innovative mashup, and has made public many data sets to facilitate the creation of data mashups: BBC, 'Government launches data mashup' <http://news.bbc.co.uk/2/hi/technology/7484131.stm> accessed 24 November 2010.

[24] This is not to say that issues of notice, consent and data retention are not important. For example, the Privacy Commissioner of Canada has published a letter to Google highlighting these concerns: Privacy Commissioner of Canada, 'Letter to Google Inc regarding the company's proposed retention plan for images collected for its StreetView application' (21 August 2009) <http://www.priv.gc.ca/media/nr-c/2009/let_090821_e.cfm> accessed 24 November 2010. Nevertheless, the greatest movement on the privacy front with Street View has been in relation to the decision of the technology giant to blur faces and licence plates that are caught on camera, and to develop a process to permit individuals to request that images be removed: Google Maps Privacy <http://www.google.com/intl/en_us/help/maps/streetview/privacy.html> accessed 24 November 2010.

private sector. Each province and territory has its own data protection legislation which is typically combined in a statute that also governs access to information.[25] Oversight of both regimes generally lies with an information and privacy commissioner.[26] The federal government has its own public sector data protection legislation. This includes the Privacy Act,[27] which is distinct from the federal Access to Information Act[28] and is overseen by the Privacy Commissioner of Canada, and the federal Personal Information Protection and Electronic Documents Act[29] (PIPEDA), which governs the collection, use and disclosure of personal information in the federally regulated private sector, inter-provincially, and in each province that does not have its own 'substantially similar' data protection legislation. It is overseen by the Privacy Commissioner of Canada.[30] Three provinces, Quebec, Alberta and British Columbia, have substantially similar private sector data protection statutes that are overseen by the Information and Privacy Commissioner of each province respectively.[31]

The federal Privacy Act defines personal information as 'information about an identifiable individual that is recorded in any form'[32] and offers a series of examples. Similar definitions are found in the freedom of information and protection of privacy statutes of the common law provinces and territories.[33] PIPEDA and its

[25] Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (British Columbia); Freedom of Information and Protection of Privacy Act, RSA 2000, c F–25 (Alberta) (Alberta FOIP Act); The Freedom of Information and Protection of Privacy Act, SS 1990-91, c F–22.01 (Saskatchewan); The Freedom of Information and Protection of Privacy Act, CCSM c F175 (Manitoba); Freedom of Information and Protection of Privacy Act, RSO 1990, c F31 (Ontario) (Ontario FOIP Act); Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56 (Ontario); An Act respecting Access to documents held by public bodies and the protection of personal information, RSQ c A–2.1 (Quebec); Right to Information and Protection of Privacy Act, SNB 2009, c R–10.6 (New Brunswick); Freedom of Information and Protection of Privacy Act, SNS 1993, c 5 (Nova Scotia); Access to Information and Protection of Privacy Act, SNL 2002, c A–1.1 (Newfoundland); Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F–15.01 (Prince Edward Island); Access to Information and Protection of Privacy Act, RSY 2002, c 1 (Yukon); Access to Information and Protection of Privacy Act, SNWT 1994, c 20 (Northwest Territories); Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20 (Nunavut).

[26] A list of all provincial and territorial oversight offices can be found on the website of the Office of the Privacy Commissioner of Canada (OPC).

[27] Privacy Act, RSC 1985, c P–21, s 2.

[28] Access to Information Act, RSC 1985, c A–1.

[29] SC 2000, c 5.

[30] The Commissioner has no order-making powers under PIPEDA, and is limited to making findings and recommendations. The legislation does, however, provide for a complainant or the Commissioner to bring a matter to Federal Court once the Commissioner's report has been issued.

[31] British Columbia's Personal Information Protection Act, SBC 2003, c 63 (PIPA BC); Alberta's Personal Information Protection Act, SA 2003, c P–6.5 (PIPA Alberta); Quebec's An Act respecting the protection of personal information in the private sector, RSQ c P–39.1, as amended (PPIPS). Each provincial Commissioner has order-making powers under their respective legislation.

[32] Privacy Act (n 27) s 3.

[33] Freedom of Information and Protection of Privacy Act, RSBC 1996 (n 25) Schedule 1; Alberta FOIP Act (n 25) s 1(n); The Freedom of Information and Protection of Privacy Act, SS 1990–91 (n 25) s 24; The Freedom of Information and Protection of Privacy Act, CCSM (n 25) s 1; Ontario FOIP Act (n 25) s 2(1); Municipal Freedom of Information and Protection of Privacy Act, RSO 1990 (n 25) s 2; Right to Information and Protection of Privacy Act, SNB 2009 (n 25) s 1; Freedom

common law provincial counterparts govern the collection, use and disclosure of 'personal information'; the common element of their definitions is that such information is 'information about an identifiable individual'.[34] This paper will focus on this common element of definitions of 'personal information'.

Data protection statutes in Canada are generally not specific as to the form that personal information may take.[35] Such information can be medical or biological data,[36] biometric data,[37] the sound of one's voice,[38] photographic or video images,[39] data,[40] or other written information. Information represented on information maps, in photographs or in the complex tapestry of images on an application like Google Street View is capable of constituting 'personal information' if it is 'about an identifiable individual'.[41]

3 The Test for Personal Information

The statutory definitions of 'personal information' have been given a fairly broad interpretation.[42] For example, in *Canada (Information Commissioner) v Canada (Canadian*

of Information and Protection of Privacy Act, SNS 1993 (n 25) s 3(1); Access to Information and Protection of Privacy Act, SNL 2002 (n 25) s 2(o); Freedom of Information and Protection of Privacy Act, RSPEI 1988 (n 25) s 1(i); Access to Information and Protection of Privacy Act, RSY 2002 (n 25) s 3; Access to Information and Protection of Privacy Act, SNWT 1994 (n 25) s 2; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994 (n 25) s 2. Most access to information statutes refer to information that is 'recorded', whereas private sector data protection legislation is more open-ended. This is perhaps because it would not be practicable to deal with access to information requests in relation to personal information that is not recorded.

[34] PIPEDA (n 29) s 2; PIPA BC (n 31) s 1; PIPA Alberta (n 31) s 1(1)(k). Each statute separately addresses the case of employees' personal information.

[35] An exception is the federal Privacy Act (n 27) s 3, which requires that personal information be 'recorded in any form'. Information that is not 'recorded' falls outside this definition. This is typical of public sector access to information and data protection legislation, most likely because it would be difficult to manage information under these regimes if it was not in recorded form.

[36] *Rousseau v Wyndowe*, 2006 FC 1312 (Federal Court (Canada)), varied on different grounds in 2008 FCA 39 (Federal Court of Appeal).

[37] *Yeager v Canada (Minister of Citizenship and Immigration)*, 2008 FC 113. See also Privacy Act (n 27) s 3.

[38] *Wansink v Telus Communications Inc*, 2007 FCA 21.

[39] *Eastmond v Canadian Pacific Railway*, 2004 FC 852.

[40] *Gordon v Canada (Minister of Health)*, 2008 FC 258.

[41] The issue of whether Google Street View images are personal information is juridically different from the issue of whether the information is *private* information. Data protection laws do not protect privacy *per se*. They give individuals a set of expectations regarding the conditions under which their personal information will be collected, used or disclosed by public or private sector actors. Because of the highly qualified nature of these expectations, the definition of personal information is fairly broad. For the purposes of a privacy rights analysis (for example, where privacy is a human right), the issue may be framed in terms of the reasonableness of any expectation of privacy an individual might have in particular information in a given context: eg *Aubry v Éditions Vice-Versa* [1998] 1 SCR 591 (Supreme Court of Canada); *Campbell v MGN Ltd* [2004] UKHL 22 (House of Lords).

[42] In *Rousseau* (n 36), Justice Teitelbaum observed that this was the first case requiring an interpretation of 'personal information' under PIPEDA. The case concerned whether notes taken by a doctor during a medical exam constituted the patient's personal information. Justice Teitelbaum found that the definition was broad enough to include this kind of information.

Transportation Accident Investigation & Safety Board),[43] a case decided under federal access to information legislation, Justice Desjardins of the Federal Court of Appeal stated that information is 'personal information' if it is:

> 'about' an individual and if it permits or leads to the possible identification of the individual. 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.[44]

This formulation gives weight to each of two elements in the definition of personal information as 'information about an identifiable individual'. This approach requires first that information be *about* an individual and secondly that the individual must be *identifiable*. Each of these elements plays a role in shaping the scope of 'personal information'.

(a) 'About'

In *Dagg v Canada (Minister of Finance)*,[45] the Supreme Court of Canada considered whether copies of building entry logs with the names, ID numbers and signatures of Department of Finance employees constituted information 'about' those employees. The employees had signed the log sheets when entering and leaving their workplace on weekends. The logs had been sought under the Access to Information Act,[46] and the release of the information was objected to on the basis that it constituted the employees' personal information. Although the Court was divided on the outcome of the case, the majority of judges accepted his statement that 'information relating primarily to individuals themselves or to the manner in which they choose to perform the tasks assigned to them is 'personal information'' '.[47] However, s 3(j) of the federal Privacy Act expressly excludes the following from the definition of 'personal information' for the purposes of the Access to Information Act:

> **3**. (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

[43] [2007] 1 FCR 203 (*Transportation* case).
[44] ibid [43].
[45] [1997] 2 SCR 403.
[46] Access to Information Act (n 28).
[47] *Dagg* (n 45) [94].

(v) the personal opinions or views of the individual given in the course of employment . . .

In the result, the court was divided on the characterisation of the information before it. A narrow majority decided that the information in the logs related to the 'position or function of the individual'[48] and was thus not 'personal information' according to s 3(j). Without this express exception from the definition of 'personal information' in the Privacy Act, this type of information would otherwise presumably be included within the scope of 'information about an identifiable individual'. This view is confirmed by the Supreme Court of Canada's subsequent decision in *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*,[49] where Justice Gonthier held that the definition of 'personal information' was meant to receive a broad interpretation that would, but for the exception in s 3(j), include the type of information set out there.[50]

Although the *Dagg* distinction could well be said to be limited only to situations involving officers or employees of a government institution where the information in question relates to their position or functions, it has surfaced in other contexts as well. As noted in the *Transportation* case, the Federal Court of Appeal made 'about' an independent consideration when it ruled that to constitute personal information, information must not only relate to an identifiable individual, but it must also be 'about' them. In that case, the court held that communications between pilots and air traffic control operators were not the personal information of the individuals involved because it was not *about* them. Rather, the information was considered to be about aircraft and air transportation issues. It is '*non*-personal information transmitted *by* an individual in job-related circumstances'.[51] For the Federal Court of Appeal, information about oneself is information which relates to fundamental privacy concepts of 'intimacy, identity, dignity and integrity of the individual'.[52]

The distinction between information 'about' an individual and information 'about' something else is also evident in cases arising under provincial legislation. In *Alberta Infrastructure*,[53] an adjudicator considered a request for access to copies of

[48] *Dagg* (n 45) [8]. Another example is found in the adjudicator's decision in *Calgary Police Service*, Alberta Office of the Information and Privacy Commissioner (Alberta OIPC), Order F2008–009 (19 August 2008) <http://www.oipc.ab.ca/ims/client/upload/Order%20F2008-009.pdf> accessed 24 November 2010. The adjudicator found that the names of government officials who filed complaints against members of the Calgary Police Service could be disclosed: 'As they were conducting government business, and there is no personal dimension to their activities, the information other than their names is not personal information at all' (at [95]). See also the Commissioner's decision in *Edmonton Police Service*, Alberta OIPC, Order F2006–030 (16 January 2008) [12] <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2432> accessed 24 November 2010.

[49] 2003 SCC 8.

[50] ibid [38].

[51] *Transportation* case (n 43) [54].

[52] *Transportation* case (n 43) [52].

[53] *Alberta Infrastructure*, Alberta OIPC, Order F2008–019 (31 July 2008) < <http://www.oipc.ab.ca/ims/client/upload/Order%20F2008-019-F39022.pdf> accessed 24 November 2010.

records relating to the sale of certain buildings from Alberta Infrastructure under Alberta's FOIP Act.[54] One of the issues raised related to whether disclosure of documents signed by officers of the companies involved could be denied because the documents contained the individuals' signatures, which constituted their personal information. The adjudicator ruled that the signatures were 'not information about these individuals, but rather, about the entities they represent.'[55] She quoted from an earlier decision of the Alberta OIPC, where the Commissioner wrote, 'a record of what a public body employee has done in their professional or official capacities is not *personal* or *about the person*, unless that information is evaluative or is otherwise of a 'human resources' nature, or there is some other factor which gives it a personal dimension'[56]

In *Calgary Police Service*,[57] another access to information decision under Alberta's FOIP Act released about a month later, the adjudicator considered whether the information that certain government employees had filed complaints with the Calgary Police Service constituted 'personal information'. He ruled that '[a]s they were conducting government business, and there is no personal dimension to their activities, the information other than their names is not personal information at all.'[58] Similarly, in In *Order PO–2750 (University of Ottawa)*,[59] the adjudicator under Ontario's FOIP Act[60] expressed the view that information about individuals in their 'professional, official or business capacity will not be considered to be "about" the individual.'[61] However, she qualified this statement by observing that some information about an individual in their professional or business capacity might still be personal information if it 'reveals something of a personal nature about the individual.'[62]

In *Re Prince Edward (County)*[63] another adjudicator under the same statute considered whether information in a letter sent by the deputy chief building/by-law enforcement officer to an individual named in the letter was the personal information of the recipient. It was argued that to be considered personal

[54] (n 25).

[55] *Alberta Infrastructure* (n 53) [32]. See also *Alberta Employment and Immigration*, Alberta OIPC, Order F2008–028 (16 July 2009) [53] <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2646> accessed 24 November 2010.

[56] *Alberta Infrastructure* (n 53) [33], citing *Alberta Labour Relations Board*, Alberta OIPC, Order F2004–026 (18 September 2006) [111] <http://www.oipc.ab.ca/ims/client/upload/F2004-026.pdf> accessed 24 November 2010.

[57] (n 48).

[58] ibid [95]. He also found that disclosure of their names in those circumstances would not unreasonably invade their personal privacy.

[59] Ontario OIPC, Order PO–2750 (6 January 2009) <http://www.ipc.on.ca/images/Findings/po-2750.pdf> accessed 24 November 2010.

[60] (n 25).

[61] (n 59) 5.

[62] ibid.

[63] Ontario OIPC, Order MO–2432 (18 June 2009) <http://www.ipc.on.ca/images/Findings/MO-2432_1.pdf> accessed 28 November 2010; [2009] OIPC No 92.

information, it had to be 'about the individual in a personal capacity.'[64] The adjudicator considered past decisions which found that, for example, information about 'the municipal location of a property and its estimated market value' was information about the property and not about its owner,[65] and that information about planning and land use issues relating to a particular property was not about an 'identifiable individual.'[66] She concluded that the letter, which discussed the Building Code in relation to the specific property, was not *about* the named individual in her personal capacity.[67]

The distinction between information 'about' an individual and information about something else is common in the access to information context. It also emerges in the private sector data protection context. The distinction was made, for example, in PIPEDA Case Summary #2001–14,[68] under the federal private sector data protection legislation. The Privacy Commissioner ruled that information about the prescribing practices of individual physicians, which was collected and sold by marketing companies to allow their clients to target their marketing efforts directly to physicians, was not the personal information of the physicians. This information was found not to be about the physicians, but rather was about their work—it was characterised as 'work product' information. This decision has been criticised,[69] and subsequent decisions suggest that the OPC may be departing from it.[70] More recently, however, some private sector data

[64] ibid 2.

[65] *Minister of Revenue*, Order 23; [1988] OIPC No 23.

[66] *Ministry of Transportation*, Order PO–1847; [2000] OIPC No 232.

[67] Order MO–2432 (n 63) 4. The record was ordered disclosed with the name and address of the recipient of the letter severed.

[68] 'Selling of information on physicians' prescribing patterns' (21 September 2001) <http://www.priv.gc.ca/cf-dc/2001/cf-dc_010921_e.cfm> accessed 3 January 2011.

[69] See, eg, Teresa Scassa, Theodore Chiasson, Michael Deturbide and Anne Uteck, 'Consumer Privacy and Radio Frequency Identification Technology' (2005–06) 37 University of Ottawa Law Review 215, 232; Paul Bigioni, 'Question: What is 'Personal Information' under the PIPEDA?' (*Lawyers Weekly*, 11 February 2005) <http://www.lawyersweekly.ca/index.php?section=article&articleid=32> accessed 28 November 2010; Bonnie Cham, 'Review of Personal Information Protection and Electronic Documents Act (PIPEDA)' (Notes for an Address, 13 December 2006) 2–3 <http://www.cma.ca/multimedia/CMA/Content_Images/Inside_cma/Submissions/2006/presentation-pipeda-en.pdf> accessed 3 January 2011.

[70] PIPEDA Case Summary #2003–220, 'Telemarketer objects to employer sharing her sales results with other employees' (15 September 2003) <http://www.priv.gc.ca/cf-dc/2003/cf-dc_030915_e.cfm> accessed 3 January 2011 and PIPEDA Case Summary # 2005–303, 'Real estate broker publishes names of top five sales representatives in a city' (31 May 2005) <http://www.priv.gc.ca/cf-dc/2005/303_20050531_e.cfm> accessed 3 January 2011. See also OPC, 'Interpretations (Personal Information)' <http://www.priv.gc.ca/leg_c/interpretations_02_e.cfm#> pt III (Applications in Different Contexts: Business and Professional Context) accessed 3 January 2011. In 2007, the federal government issued its response to a report of the Standing Committee on Access to Information, Privacy and Ethics regarding proposed reforms to PIPEDA. One of these had recommended an amendment to the law to expressly exclude 'work product information' from the definition of personal information. The government acknowledged a need to consult further on the issue of how work product information can be accommodated in a manner that poses the least degree of risk to privacy protection.' See Industry Canada, 'Government

protection decisions have suggested that personal information must be 'about' an individual in that it reveals something of a personal character.[71]

Many of the cases discussed above were decided under access to information legislation. The fact that these cases distinguish rather broadly between information 'about' an identifiable individual and information 'about' something else must be treated with some caution in the data protection context. The overarching goal of access to information legislation is to enhance government accountability by giving the public access to government documents or records.[72] Access to information legislation typically contains an exception for disclosure of information that would result in an undue invasion of the privacy of third parties. The definitions of personal information advanced in access to information cases must be seen as part of a consideration of the circumstances in which there should be derogation from the general goals of accountability and public access to government records. The definition of personal information in this context may serve different goals than private sector data protection legislation.

In the federal context, it is clear that s 3(j) of the Privacy Act influenced the definition of 'personal information' in *Dagg*. Further, the *Transportation* case,[73] as an access to information case, should not necessarily be seen to mandate an approach to 'personal information' that requires a division between information 'about' an individual and information 'about' something else. In that case, the Federal Court of Appeal cautioned that *Dagg* related to the interpretation of a statute that contained a specific exception for information about a position, and that the views expressed might not be applicable more widely in cases about personal information under other statutes. In *Englander v Telus Communications Inc*, the Federal Court of Appeal also cautioned that the purpose of PIPEDA is 'altogether different'[74] from that of the federal *Privacy Act*, and that its interpretation might be guided by different considerations.

While under private sector data protection statutes there have been findings that information must be 'about' an individual in their personal capacity, these decision-makers have shown a greater willingness to find this link in relatively

Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics, Statutory Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)' (17 October 2007) <http://www.ic.gc.ca/eic/site/ic1.nsf/eng/h_02861.html> accessed 28 November 2010. Proposed amendments to PIPEDA are contained in Bill C–29, Safeguarding Canadians' Personal Information (Third Session, Fortieth Parliament, 59 Elizabeth II, 2010), s 6 of which deals with work product information by exempting it from consent requirements for collection, use or disclosure in specified circumstances.

[71] In Case Summary #2003–220 (n 70), the Assistant Privacy Commissioner of Canada accepted that information could be both about a person's employment, and about them personally. See also Case Summary # 2005–303 (n 70); PIPEDA Case Summary #2006–349, 'Photographing of tenants' apartments without consent for insurance purposes' (24 August 2006) <http://www.priv.gc.ca/cf-dc/2006/349_20060824_ e.cfm> accessed 3 January 2011.

[72] See, eg, the statement of purpose in the Access to Information Act (n 28) s 2.

[73] (n 43).

[74] 2004 FCA 387 [38].

small things. Thus, for instance, the selling price of a home was considered to reveal something about an individual's ability as a negotiator.[75] It is therefore possible that the threshold for 'personal information' is slightly lower in data protection legislation than it is under access to information laws. Whether this is appropriate or is likely to raise difficulties in the context of geographic information is considered in Part 5 below.

(b) Identifiable individual

Information must be about an *identifiable individual* for it to be personal information. Some geographic information, such as a person's home address, is obviously about an identifiable individual. GI that is personal information can be in any form, and can include reports, photographs, video or data communicated from a tracking device, so long as the individual revealed in or by this data or imagery is identifiable. Identifiability, however, does not require an immediate or obvious link to the individual. For example, the OPC takes the position that '[t]racking information collected from a Global Positioning System (GPS) placed in company vehicles is personal information, since the information can be linked to specific employees driving the vehicle.'[76] Although the link may not be overtly made, if it is possible to make the link, the information is personal information. For example, the OPC also takes the view that RFID data and IP addresses may be personal information so long as they are associated with an identifiable individual in some record that can be consulted.[77] This approach is evident as well in the decision from Alberta's OIPC in *Leon's Furniture*, where a driver's licence number and a car licence plate number were both found to be information about an identifiable individual since one could identify the individual associated with each number by consulting the appropriate database.[78]

The issues of identifiability in the above cases are relatively straightforward, as the dots connecting the individual to the information are exactly where and what one would expect them to be. A drivers' licence number must be linkable to an identifiable individual, or it is not capable of serving its function. Similarly, for an employer, information about the location of a vehicle can easily and obviously be linked to the employee who is driving it. Compilations of data that include a

[75] PIPEDA Case Summary #2009–002, 'Realtor advertises purchase price of condominium in trade publication without buyer's consent' (20 February 2009) <http://www.priv.gc.ca/cf-dc/2009/2009_002_0220_e.cfm> accessed 3 January 2011.

[76] OPC, 'Interpretations (Personal Information)' (n 70), citing PIPEDA Case Summary #2006–351, 'Use of personal information collected by Global Positioning System considered' (9 November 2006) <http://www.priv.gc.ca/cf-dc/2006/351_20061109_e.cfm> accessed 3 January 2011.

[77] OPC, *Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices* (Consultation Paper, March 2008) <http://www.priv.gc.ca/information/pub/rfid_e.pdf> accessed 3 January 2011.

[78] Alberta OIPC, Order P2008–004 (27 August 2008). See also *Home Depot of Canada Inc*, Order P2007–016 (20 March 2008).

geographic component may present more challenging issues, as the identification of individuals may be indirect and accomplished through the use of sources outside the data set. In this context, it is useful to look at two key cases in order to consider when such collections of data can be said to reveal personal information.

The leading case on identifiability in Canada is the decision in *Ontario (Attorney General) v Pascoe*.[79] In this case, a reporter had applied under Ontario's FOIP Act for disclosure of the medical procedures that had been charged to the government by Toronto's highest billing general practitioner in 1998–99. Disclosure was granted. Judicial review of the decision of the Commissioner was sought, *inter alia*, on the basis that the information disclosed was personal information.

Under Ontario's FOIP Act, 'personal information' is defined as 'information about an identifiable individual'. Where information is personal information, the head of an institution may not disclose it unless to do so 'does not constitute an unjustified invasion of personal privacy.' The Ontario Court of Appeal essentially confirmed the decision of the Divisional Court which sat in review of the decision of the Ontario Information and Privacy Commissioner. The Divisional Court had noted that the records sought by the applicant did not expressly name the physician. However, it observed that 'it is common ground that the records may themselves, or in combination with other information, identify the individual even if he or she is not specifically named.'[80] The Divisional Court set out what it considered to be the accepted test: 'If there is a *reasonable expectation* that the individual can be identified from the information, then such information qualifies under subsection 2(1) as personal information.'[81] It accepted that identification could occur through matching with information from a wide range of sources, including individual knowledge. It noted that '[a] person is also identifiable from a record where he or she could be identified by those familiar with the particular circumstances or events contained in the record.'[82]

In 2008, the Federal Court of Canada considered a similar issue arising under the federal Access to Information Act in *Gordon*.[83] Justice Gibson was faced with an application for judicial review of the decision of the Minister of Health, which declined to disclose the field titled 'province' in the Canadian Adverse Drug Reactions Information System (CADRIS) database. The applicant Gordon, a journalist, had made an access to information request to Health Canada seeking access to and a copy of the CADRIS database. The database contained information regarding suspected adverse reactions to health products in Canada. The information came from voluntary reports, as well as reports by drug

[79] (2002) 22 CPR (4th) 447 (Ont CA), affirming *Ontario (Attorney General) v Ontario (Information and Privacy Commissioner)* [2001] OJ No 4987, 16 CPR (4th) 460 (Ont Div Ct) (*Pascoe*) and Order P–230 [1991] OIPC No 21.

[80] *Pascoe* (Ont Div Ct) (n 79) [14].

[81] ibid (emphasis added). This test is drawn from Order P–230 [1991] OIPC No 21.

[82] ibid [15].

[83] (n 40).

manufacturers. The database contained about 125 data fields. The Minister provided access to 82 data fields, but refused access to 12 other fields on privacy grounds. The only field in dispute at the time of the Federal Court hearing was that involving 'province'.

The information relating to 'province' had been withheld because of a concern that if it were disclosed, it might reveal the identities of specific individuals. The decision not to disclose was made under s 19 of the Access to Information Act,[84] which prohibited the disclosure of any records containing personal information without the consent of the individual to whom it relates, unless the information is publicly available or unless the disclosure is in accordance with s 8 of the Privacy Act.[85]

Justice Gibson first considered whether the field of 'province' was personal information. Citing the *Transportation* case,[86] he noted 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.'[87] While the Federal Court of Appeal in the *Transportation* case had cited *Pascoe* in support of this test, Justice Gibson went on to adopt as correct the test for identifiability proposed by the OPC, which had intervened in the case. According to this formulation, '[i]nformation 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.'[88] He was satisfied that if the information relating to province were combined with other available information, it

> would substantially increase the possibility that information about an identifiable individual that is recorded in any form would fall into the hands of persons seeking to use the totality of information disclosed from the CADRIS database, in conjunction with other publicly available information, to identify 'particular' individuals.[89]

Justice Gibson appears to accept that the sources that could be used to identify individuals in combination with the disclosed information could include virtually anything, including the knowledge of hospital workers or neighbours of victims.[90]

[84] (n 28).

[85] ibid s 19. S 8 of the Privacy Act (n 27) provides a series of exceptions to the bar on disclosure. In this case, the most relevant exception was where 'the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure' (s 8(2)(m)(i)).

[86] (n 43).

[87] *Gordon* (n 40) [32]–[33].

[88] ibid [34] (emphasis added). Note that the 'serious possibility' test was previously applied by the OPC: PIPEDA Case Summary #2007–372, 'Disclosures to data brokers expose weaknesses in telecoms' safeguards' (9 July 2007) <http://www.priv.gc.ca/cf-dc/2007/372_20070709_e.cfm> accessed 3 January 2011.

[89] ibid [43].

[90] *Gordon* (n 40) [43]. Gibson J accepted affidavit evidence that discussed the possibility of re-identification.

It is unclear whether, or to what extent, *Gordon* departs from *Pascoe* to set a new standard under federal legislation. Arguably, less information will be considered 'personal information' using a 'reasonable expectation' standard as compared to the 'serious possibility' standard. As will be seen below, the reasonable expectation standard turns, not on the *possibility* that re-identification could occur, but rather on the likelihood, in all the circumstances, that it will take place.[91]

In spite of the apparent differences, it is difficult to assess the degree of practical difference between *Gordon* and *Pascoe*, because of the facts in each case. In *Pascoe*, the Commissioner had dismissed the objections of the Ministry that the information could lead to the identification of the physician in question largely because the Ministry had not done enough to establish the 'reasonable expectation' of identification. The reviewing courts found this decision to be reasonable. According to the Divisional Court:

> The Ministry, apart from its small cell count finding, did not proffer any submissions establishing a nexus connecting the record, or any other information, with the affected person. Any connection between the record and the affected person, in the absence of evidence, is merely speculative. The Ministry made no submissions explaining its small cell count finding or showing how it applied to the facts of this case. No other information was identified by the Ministry or by the affected person that could link the record to an identifiable individual.[92]

In *Gordon*, by contrast, Justice Gibson was clearly influenced by evidence that journalists had already managed to identify one victim by matching the adverse drug reaction information with publicly available obituary information.

It is important to note as well that none of the courts or adjudicators who have considered the issue of when information is about an *identifiable* individual have specified the 'test person' from whose perspective the evaluation should be made. *Pascoe*[93] requires a 'reasonable expectation' that identification could take place, but it is unclear whether this is from the point of view of an expert in data matching, a person who seeks out information for a living such as a journalist, or simply an ordinary individual. Kosseim and El Emam observe:

> Canadian thresholds don't require application from any particular perspective (for example, a highly sophisticated expert, a motivated intruder, or an average layperson). Nor do Canadian thresholds expressly reference the level of resources, time, or effort necessary to re-identify individuals.[94]

[91] Under New Brunswick's Personal Information Protection Act (n 33) s 1(3)(c), an individual is considered identifiable if 'information does not itself include the name of the individual or make his or her identity obvious but is likely in the circumstances to be combined with other information that does.' 'Likely in the circumstances' would appear closer to a 'reasonable expectation' test.

[92] *Pascoe* (Ont Div Ct) (n 79) [20].

[93] *Pascoe* (Ont Div Ct) (n 79).

[94] Patricia Kosseim and Khaled El Emam, 'Privacy Interests in Prescription Data, Part II' (March–April 2009) IEEE Security and Privacy 75, 75.

The perspective to be adopted is crucial, as it has great bearing on whether there is a 'reasonable expectation' or 'serious possibility' that an individual might be identifiable.

There has been little federal case law to date that considers the threshold for re-identification set out in *Gordon*[95]. PIPEDA *Case Summary* 2007–372[96] dealt with the use of pretexting to obtain call records of cell phone customers. Pretexting involves contacting an organisation to obtain information about individuals by pretending to be someone who is entitled to access this information. It was argued that a particular cell phone holder was not identifiable from the call records. The Assistant Privacy Commissioner of Canada (APC) disagreed, stating:

> Had Locatecell.com or the journalist (or anyone else for that matter) called everyone on the call record list, there was indeed a serious possibility that they would be able to piece together enough information so as to eventually be able to ascertain the correct identity of the BlackBerry holder.[97]

The APC was prepared to find a serious possibility without requiring evidence to demonstrate how the dots could be connected.

The *Pascoe* standard by contrast, appears to place a heavier evidentiary burden on the party arguing that there is a reasonable expectation of identification. For example, in *Minister of Community Safety and Correctional Services*[98] the adjudicator considered an appeal from a denial of access to certain information sought by a journalist. The journalist had requested a 'data snapshot' of inmates serving sentences of up to two years less a day in Ontario prisons. The data he sought was the length of sentence being served for each inmate as well as the postal code on record for each inmate. The Minister indicated that it would provide only the first three digits of each postal code associated with the aggregate sentence length for that code. The adjudicator considered whether the information being sought was 'personal information' within the meaning of the Ontario FOIP Act[99] and according to the standard set out in *Pascoe*. The Minister had argued that disclosing the last three characters in each postal code could permit the identification of individuals when matched with the other data. This would be particularly likely in urban areas, where a single apartment building might be assigned its own postal code. The Minister also maintained that the data being sought could be matched with other publicly available data so as to identify individuals.

The adjudicator concluded that the full postal code information on these facts did not constitute personal information using the *Pascoe* 'reasonable expectation' of re-identification test. She found that the fact that an individual *might* be

[95] *Gordon* (n 40).
[96] (n 88).
[97] ibid.
[98] Ontario OIPC, Order PO–2726 (22 October 2008).
[99] (n 25).

identified from the data if someone conducted a 'laborious search of newspaper articles' was too remote to satisfy the requirement of a reasonable expectation of identifiability.[100]

The issue of whether partial address information can constitute personal information has been considered in other cases. In *Order PO–2347*,[101] the adjudicator ruled that where the unit numbers of apartments in a larger building were stripped from the address information, insufficient information remained to identify specific residents. In another decision[102] an adjudicator found that postal codes did not constitute personal information as there was no other information that could allow the postal code information to identify a specific individual. The decision might be otherwise where postal code data is linked to a great deal of information about individuals. In a British Columbia investigator's report, the volume of information at issue combined with the fact that some individuals lived in very small communities where identification would be greatly facilitated, led to the conclusion that the postal code information was 'personal information', and that only the first three digits should be disclosed.[103]

In Ontario the *Pascoe* test is well-established, and *Pascoe* has gained some traction in other provinces as well.[104] It is less clear whether at the federal level the *Gordon* test will prevail. It also remains uncertain whether 'serious possibility' sets a lower threshold for personal information than 'reasonable expectation'. Certainly, 'serious possibility' appears merely to require a party to identify something more than a remote possibility of re-identification. 'Reasonable expectation' focuses instead on whether any possibility is likely to be realised. Yet at the end of the day, the standards might not be so far apart. The 'seriousness' of a possibility may be found to turn on issues similar to those which have been informed a 'reasonable expectation,' and it is possible that in both cases some evidence may be required

[100] She also found that with this particular set of data, the chances of identifiability were remote because the data had already been generalised to avoid identifiability. The data snapshot was from 2007, but was not otherwise associated with a specific date. In addition, the adjudicator noted that: 'the number of individuals to which each entry in the aggregate sentence length column refers is unknown; and there could be one or more individual's sentences associated with each postal code.'get citation and pinpoint. For research on the identifiability of individuals based on postal code information, see Latanya Sweeney, 'k-Anonymity: A Model for Protecting Privacy', (2002) 10 *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems* 557; Khaled El Emam, Ann Brown and Philip Abdel Malik, 'Evaluating Predictors of Geographic Area Population Size Cut-offs to Manage Re-identification Risk' (2009) 16(2) *Journal of the American Medical Informatics Association* 256.

[101] *Ontario Rental Housing Tribunal*, Order PO–2347, 25 November 2004.

[102] *Ontario Lottery and Gaming Corporation*, Order PO–2131, 20 March 2003.

[103] *Investigation Report P97–009*, Office of the Information and Privacy Commissioner of British Columbia (BC OIPC), 17 March 1997.

[104] Eg, the test is relied upon in Newfoundland and Labrador, Report 2007–008 (Eastern Regional Integrated Health Authority); in British Columbia in *Order 03–42: Ministry of Health Services* (17 December 2003); in Nova Scotia in *FI–00–109: Re Nova Scotia (Department of Justice)* (12 January 2001), and in Prince Edward Island in *Order No 05–005: Re Workers Compensation Appeal Tribunal* (19 April 2005) s VI.

to establish either the serious possibility or the reasonable expectation.[105] Yet the unsettled nature of the test under federal legislation is problematic, as it makes it difficult for business or government to predict the circumstances in which information will be considered to be personal information.[106]

Both tests also pose challenges in a context where the nature and volume of available data sets that could be used in matching continues to increase, and can change rapidly over time. Indeed this is likely to be a significant problem in both public and private sectors when trying to anticipate whether the disclosure of a set of data—for example, the presentation of a data map—will amount to a disclosure of personal information. Even if the department or company making the disclosure is careful to test whether individuals can be identified by matching the disclosed data with other available data so as to identify particular individuals, the kind, quality and volume of 'other' sources of data is constantly changing. Further, the *Gordon* test at least appears to anticipate that neighbours or coworkers of individuals, who might have access to information not widely shared, can be relevant data sources.

Cases like *Minister of Community Services* attempt to qualify the 'reasonable expectation' that information could be linked to identifiable individuals by factoring in considerations such as the general accessibility of other data sources, and the cost of accessing them. Yet these are also moving targets. Data sets that today may only accessible to those who are prepared to do a great deal of footwork or who are prepared to pay for commercial accounts, may at some not too distant time in the future become more freely publicly accessible, or the costs of searches may drop dramatically. Commercial and public sources may also expand, making cross-referencing or the searching through multiple records at one time quick and easy. What constitutes 'personal information' in this rapidly shifting data context can change from one day to the next.

4 Re-identification Risk Approach

Given the rapidly changing data environment, are there other ways to address what constitutes personal information? Some sets of data may be generalised in such a way that specific individuals are not capable of being associated with it. In fact, cases

[105] In *Gordon* (n 40), there was evidence of actual re-identification. Other Ontario cases that have required evidence of a nexus include: *Order P–1389: Re Ontario (Ministry of Health)* (8 May 1997); *Order PO–1880: Re Ontario (Ministry of Health and Long Term Care)* (15 March 2001); and *Order PO–2726: Re Ontario (Ministry of Community Safety and Correctional Services)* (22 October 2008) [2008] OIPC No 186.

[106] It is interesting to note that a somewhat different standard is incorporated into Ontario's Personal Health Information Protection Act, SO 2004, c 3, sch A (PHIPA). PHIPA applies specifically to personal health information. The Act offers a detailed list of types of health information that are covered. This information is 'personal' health information when it is 'identifying information about an individual'. 'Identifying information' is separately defined as 'information that identifies an individual or for which it is *reasonably foreseeable in the circumstances* that it could be utilised, either alone or with other information, to identify an individual' (s 4(2), emphasis added).

like *Gordon* and *Pascoe* deal largely with the degree of generalisation that is required in order to protect individuals from being identified from a set of data. It is frequently the case with GIS that generalised data is placed in a geographical context. In such a context, a piece of GI that is not itself personally identifying may convert other data into personal information if it can be linked with that data in such a way that it becomes information about an identifiable individual. Thus a postal code may be shared by a cluster of houses, but when combined with other data such as age and sex, it may permit the identification of a specific individual.[107]

Because of the extreme sensitivity of personal health information and the value of this information in medical research, considerably more work has been done on deidentification and re-identification of personal information in the health care context.[108] In the deidentification/re-identification literature related to health information, a different standard emerges from those in *Pascoe* and *Gordon*. El Emam and others, for example, argue that what is required in the context of health data for research is a risk/benefit analysis.[109] In other words, the risk of re-identification is measured against the anticipated benefits of the use of the information in the proposed research. In the private sector data protection context, while risks of disclosure may be evident, benefits—other than for the private sector company providing the data—may be less compelling. Thus, for example, a risk/benefit analysis is more difficult to prescribe in the context of applications like Google Street View, which incidentally collects and discloses personal information about identifiable individuals captured by passing cameras. Nevertheless, it might still be argued that the risk that some individuals may be identifiable in Google Street View may not outweigh the economic and social benefits of this tool.

Access to information legislation also balances privacy interests against a broader public interest. For example, Ontario's FOIP Act[110] s 21(1)(f) provides that the head of an institution shall refuse to disclose personal information to anyone other than the person to whom it relates unless 'the disclosure does not constitute an unjustified invasion of personal privacy.' Section 21(2) sets out criteria to guide a decision-maker on this point. The factors to consider include whether:

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Ontario and its agencies to public scrutiny;
(b) access to the personal information may promote public health and safety;

[107] See, eg, Sweeney (n 100).
[108] See, eg, Khaled El Emam and others, 'Pan-Canadian De-Identification Guidelines for Personal Health Information' (Prepared for the OPC, April 2007) <<http://www.ehealthinformation.ca/documents/OPCReportv11.pdf> accessed 3 January 2011; El Emam, Brown and Abdel Malik (n 100); Timothy Caulfield and Nola M Ries, 'Consent, Privacy and Confidentiality in Longitudinal Population Health Research: The Canadian Legal Context', (2004) Health Law Journal 1.
[109] El Emam, Brown and Abdel Malik (n 100).
[110] (n 25).

(c) access to the personal information will promote informed choice in the purchase of goods and services;
(d) the personal information is relevant to a fair determination of rights affecting the person who made the request;
(e) the individual to whom the information relates will be exposed unfairly to pecuniary or other harm;
(f) the personal information is highly sensitive;
(g) the personal information is unlikely to be accurate or reliable;
(h) the personal information has been supplied by the individual to whom the information relates in confidence; and
(i) the disclosure may unfairly damage the reputation of any person referred to in the record.

The disclosure of certain types of personal information is considered to presumptively constitute an unjustified invasion of personal privacy. This includes medical or psychiatric information, employment or educational history and certain types of financial information.[111] Such criteria can be useful in managing re-identification risk in the disclosure of sets of data that might lead to the identification of individuals; they might also be useful in determining when, on a harm/benefit analysis the harm that might flow from identification of a few individuals is not significant enough to warrant limiting the deployment of the data product or service.

Because public sector data protection legislation is often a companion piece to legislation promoting access to information in the hands of government for the broader public interests of accountability and transparency, these balancing frameworks tend to be integrated within the legislation. Private sector data protection legislation seeks to balance the needs of private sector organisations with the interests of individuals, but the interests of organisations are more diffuse, and more oriented towards a private rather than public benefit.[112] As a result, private sector data protection legislation tends not to foresee this kind of risk/benefit or harm/benefit analysis. It is true that in Canada such statutes tend to limit an organisation's ability to collect, use or disclose personal information to only those 'purposes that a reasonable person would consider appropriate in the circumstances.'[113] Yet this overall reasonableness yardstick supplements rather than provides an exception to the other normative provisions of the legislation. The consequence is that once information is found to be 'personal information',

[111] See Ontario's FOIP Act (n 25) s 21(3).
[112] The Federal Court of Appeal in *Englander* (n 74) [38], emphasised the different purposes served by public and private sector data protection statutes, in particular that '[t]here are, therefore, two competing interests within the purpose of the PIPED Act: an individual's right to privacy on the one hand, and the commercial need for access to personal information on the other.'
[113] PIPEDA (n 29) s 3; PIPA Alberta (n 31) s 3 refers to the collection, use and disclosure of information 'for purposes that are reasonable'; PIPA BC (n 31) s 2 refers to the collection, use and disclosure of information 'for purposes that a reasonable person would consider appropriate in the circumstances.'

the normative provisions apply unless one of the other broad exceptions from the application of the legislation is available. This is perhaps why, in the case of Google Street View, the argument has been advanced that it pursues either journalistic or artistic purposes and is thus exempt from the application of PIPEDA altogether.[114]

5 GI as Personal Information

Some illustrations may be helpful in exploring the circumstances in which GI may become personal information. Google Street View, which supplements Google Maps with video camera footage of streets, has raised concerns about the privacy of individuals captured on camera.[115] Where individuals are identifiable from the footage, the record of their presence, appearance, associations or activities in a particular space can amount to personal information. In response to concerns expressed by the Privacy Commissioner of Canada regarding Street View's planned deployment in Canada, Google has agreed to blur faces so as to render them unidentifiable. They have also agreed to do the same with car licence plates.[116] As a licence plate can be linked to the registered owner of the vehicle, this too can be information about an identifiable individual.[117]

It is unlikely that blurring faces and licence plates will resolve all data protection concerns involving Street View, especially if one follows either the *Gordon* or *Pascoe* tests. For example, where house numbers are visible, street addresses can be traced to individual owners in the same way as licence plate numbers. Thus, an image of a house and yard visible on Street View may constitute information about an identifiable individual if the individual can be identified by consulting other sources such as a phone book or cadastral registry. While street address information linked to the name of an individual is the kind of information already

[114] PIPEDA, for example exempts from its application the collection, use or disclosure of personal information where it is exclusively for 'journalistic, artistic or literary purposes'. Comparable exceptions are found in PIPA BC (n 31) s 3(2)(b); and PIPA Alberta (n 31) s 4(3)(b). Google has advanced the exception for both artistic (based on the nature of photographs as 'artistic works') and journalistic purposes exceptions. See Sarah Schmidt, 'Privacy not protected on Google Street View, MPs Told' *The National Post* (22 October 2009) <http://www.nationalpost.com/news/story.html?id=2133506> accessed 3 January 2011. For a discussion of the scope and impact of this exception, see Teresa Scassa, 'Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets, and Information Maps', (2010) 35 Queen's Law Journal 733.

[115] For example, in June 2009, the House of Commons Standing Committee on Access to Information, Privacy and Ethics held hearings which considered, among other things, the privacy implications of Google Street View. Prior to that, the Federal Privacy Commissioner had issued a statement expressing her concerns over this application: 'Privacy Commissioner Seeks Information about Street Level Photography Available Online' (11 September 2007) <http://www.priv.gc.ca/media/nr-c/2007/an_070911_e.cfm> accessed 25 November 2010.

[116] Tamsyn Burgmann, 'Google to blur faces in Canadian Street View' *The Star* (Toronto, 5 April 2009) <http://www.thestar.com/article/614077> accessed 3 January 2011.

[117] *Leon's Furniture Ltd* (n 78).

available in publicly available records such as telephone directories, the Street View image may contain other personal information, including objects in front of the house or cars in the driveway. In combination, this information may reveal details about a person's life, tastes, habits or associates.[118] As for blurring faces, it is entirely possible to recognise individuals from attributes other than their faces—and their geographical location may combine with these attributes to reinforce the identification. In a recent access to information decision involving the Edmonton Police Service, the adjudicator refused to order the release of a video showing an alleged assault by police on a man, even with the faces blurred. He found that it would be still be possible to identify the individuals through other publicly available sources, such as reports of the incident, and that it might even be possible to identify an individual based on his clothing.[119] It would seem that for information to be about an identifiable individual, the individual need only be identifiable to one person. That was certainly the view of the adjudicator in the case involving the Edmonton Police Service mentioned above. He wrote: 'An individual does not have to be identifiable by every person reviewing a particular record in order for there to be personal information about that individual; the individual needs only to be identifiable by someone'.[120] Other case law suggests that only identifiability need be established, not proof that actual identification has taken place. In a finding under PIPEDA, for example, the APC found that photos of a tenant's apartment combined with their address rendered them identifiable, even if identification had not yet taken place.[121]

The importance of geography as an identification tool requires some limits to be placed on the concept of the identifiable individual. An illustration of the problem is offered where information in a geographical context that is about someone or something can also be associated with other individuals who can be linked to proximate locations. For example, the Toronto Star Map of the Week service produced a map that showed the precise locations of marijuana grow-operations that had been uncovered by police.[122] While the information about the seized properties was part of the public record, the graphic display of this information online might change both its character and its impact. For example,

[118] Eg in Case Summary #2006–349 (n 71) the APC found that photographs of the state of walls or the condition of a kitchen or bathroom 'revealed information about the unit dweller and his or her standard of living. It might show whether they are tidy or not, whether they can afford expensive media equipment or not, whether they love music, art or cooking.'

[119] *Re Edmonton (Police Service)*, Alberta OIPC, Order F2008–020, [2009] AIPCD No 8 (18 March 2009) <http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2425> accessed 3 January 2011.

[120] ibid [30].

[121] Case Summary #2006–349 (n 71).

[122] Patrick Cain, 'Map of the Week: Grow Operations' *The Star* (Toronto, 19 February 2009) <http://thestar.blogs.com/maps/2009/02/map-2008-marijuana-grow-operations———marijuana-grow-op-busts-in-toronto-were-down-in-2008-at-145-compared-t.html> accessed 3 January 2011.

by combining the map information with other publicly available information, we may learn that John Smith lives next door to a former 'grow operation'. This may have an impact on John Smith's ability to sell his house or to obtain what would otherwise be market value. This is ever more the case where the map is used to assist people in their choice of neighbourhood. Yet while the use of this information may have an impact on John Smith, it is not clear that this fact alone makes it his personal information. To give another example, a published map that indicates the location of flood plains based on the processing of a variety of data may have an impact on the insurance premiums of those who can be identified as living within the specified areas. Seen in one light, the information about the precise boundaries of the flood plain can translate into the information that 'Jane Smith lives on a flood plain'.

The answer to this problem may lie in the case law that has interpreted personal information to mean information that reveals something of a more 'personal' character—in other words, personal information is not just linked to an identifiable individual but is *about* the person in some personal capacity.[123] For example, as noted above, there are cases that have found that some information that can be linked to identifiable individuals is not 'about' them, but about something else.[124] It might be possible, therefore, to find that the information on a flood plain map is not also the personal information of those whose homes are located on the plain either because it is not *about* them as individuals; in other words, it is not information with a sufficiently personal character.

Nevertheless, the situation is not crystal clear. The APC has recently stated that 'information about property is personal information if it reveals something of a personal nature about an individual'.[125] That case involved the purchase price of a condominium combined with its address, which in turn could be linked to the purchaser. The APC found that the personal information revealed by the purchase price information could include characteristics such as the ability to pay such a price or the purchaser's effectiveness in bargaining.[126] While this is admittedly more personal than the fact that a person lives on a flood plain, it is still nothing more than an inference. The information that someone lives on a floodplain could lead to the inference that she is a less than diligent purchaser—information that is at least as personal as the fact that someone is good at bargaining.

[123] This is certainly true in the constitutional context. In *R v Plant* [1993] 3 SCR 281, 293 (Supreme Court of Canada), it was held that the privacy right component of s 8 'should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state.' This biographical core contains that information 'which tends to reveal intimate details of the lifestyle and personal choices of the individual.'

[124] *Transportation* case (n 43). See also *Alberta Labour Relations Board*, Alberta OIPC, Order F2004–026, [111]; *Alberta Infrastructure*, Alberta OIPC, Order F2008–019; *Calgary Police Service*, Alberta OIPC, Order F2008–009.

[125] Case Summary #2009–002 (n 75) [2009] CPCSF No 2.

[126] ibid.

In another complaint under PIPEDA, the Assistant Commissioner found that a property appraisal carried out by a bank was the personal information of the bank's customer, the property owner. She found that 'since the property was in the complainant's name, the information relating to the property, including its market value, was his personal information'.[127] There was no discussion of this being because the information in the appraisal would reveal things of a personal nature about the owner, although one would presume that certain inferences might be drawn. Yet inferences can be drawn from all kinds of information. It is not clear that the two property cases can easily be reconciled with the flood plain example. Perhaps the answer is that by following the reasoning in these cases one would conclude that the flood plain information is personal information. Yet to do so might open up the definition of 'personal information' to an unworkable extent.

The distinction between personal information and inferences is considered by the Supreme Court of Canada in *R v Tessling*.[128] This was a case under s 8 of the *Canadian Charter of Rights and Freedoms*,[129] which protects the right to be free from unreasonable search or seizure. This was a privacy, rather than a data protection, case, although the reasoning on the specific point of inferences is useful in the data protection context. In *Tessling*, the police had flown over the house of the accused, using Forward Looking Infrared technology to produce an image of the heat emanating from the house. The amount of heat escaping from the building was more than would be expected in a dwelling under ordinary use, and was consistent with the heat required for a marijuana grow operation. A search warrant was obtained in part on the basis of this information. The accused argued that the fly-over constituted an unreasonable search and seizure as it violated his privacy rights linked to his home. The Supreme Court of Canada disagreed. The Court found that the heat signature of a home was not personal information because it did not reveal anything in particular about what was going on inside the home. It merely permitted inferences to be drawn when that information was combined with other available information. Although the case has been criticised,[130] the distinction made by the Court between personal information and inferences is an important one. The difficulty is, of course, in separating out those inferences to which one is inevitably led (and thus constitute personal information) and those

[127] PIPEDA Case Summary #2008–390, 'Residential Property Appraisal Documents are Owners' Personal Information' <http://www.privcom.gc.ca/cf-dc/2008/390_20080507_e.cfm> accessed 3 January 2011.

[128] 2004 SCC 67 (Supreme Court of Canada).

[129] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act 1982, in the Canada Act 1982 (UK), c 11, sch B pt I.

[130] See, eg, Ian Kerr and Jena McGill, 'Emanations, Snoop Dogs and Reasonable Expectations of Privacy' (2007) 52 Criminal Law Quarterly 392, 431; Renée M Pomerance, 'Shedding Light on the Nature of Heat: Defining Privacy in the Wake of R v Tessling' (2005) 23 Criminal Reports (6th) 229, 233; James AQ Stringham, 'Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8?' (2005) 23 Criminal Reports (6th) 245, 251; Steve Coughlan and Marc S Gorbet, 'Nothing Plus Nothing Equals . . . Something? A Proposal for FLIR Warrants on Reasonable Suspicion' (2005) 23 Criminal Reports (6th) 239.

which are just one of an array of inferences which may be drawn from the information.

6 Geodemographic Data

The compilation and use of geodemographic information presents a challenging issue for data protection regimes. Geodemographic data places demographic information—information about a population—in a geographic context. In some cases, geodemographic information is quite general—for example, a map might show, in different colours, average household incomes across the country generalised to provinces, counties or cities.[131] This is not particularly fine-grained geodemographic data—it would be impossible to identify the household incomes of particular individuals from such a generalised map. However, depending on the nature of the demographic data and the fine grain of any geographic co-ordinates, the identification of specific individuals associated with the data may be possible. Issues of deidentification and re-identification, discussed above, are important in determining when individuals might be identifiable from geodemographic data.[132]

A further issue about geodemographic data (and indeed, about some forms of GI) arises when generalised information about a population or a region is linked to specific individuals who live in that area. For example, in a recent PIPEDA complaint, the Canadian Internet Policy Public Interest Clinic (CIPPIC) objected to the practices of a marketing company. This company took aggregate demographic data from Statistics Canada sorted according to census dissemination areas, and then matched that information with the individual households associated with that area. The company obtained the information about names and addresses from telephone directories, and used certain processes to infer gender and ethnicity where possible. Thus for example, a particular name in a telephone directory might be assumed to be that of a woman of Irish origin. This information would in turn be matched with geodemographic information that might indicate, for example, that the average income for people sharing her postal code is $100,000 per year. This information would be sold to companies seeking sets of data about particular customers who fit the target profile for their product or services.

Viewed from one angle, the resulting lists consist of personal information. The person presumed to be a woman of Irish descent and with an annual income of approximately $100,000 is identified by name and address. The individual might

[131] See, eg, maps offered by the US Centre for Disease Control (n 5). For a non-governmental source of mapped health data, see the public health data maps prepared for The Star, 'Map of the Week': <http://thestar.blogs.com/maps/public_health/> accessed 25 November 2010.

[132] Sweeney (n 100); John S Brownstein, Christopher A Cassa and Kenneth D Mandl, 'No Place to Hide—Reverse Identification of Patients from Published Maps' (2006) 355 New England Journal of Medicine 1741.

not be female, might be of some other ethnicity, or might earn considerably more or less than the assumed amount. Yet information does not need to be accurate to constitute personal information,[133] and the compiled information would not have a commercial value if it did not achieve a certain generalised level of accuracy. Since personal information is 'information about an identifiable individual', once a person's name is linked to information and decisions (such as the decision to mail financial investment information or advertisements for luxury cars) are taken based on this information, then there is a strong argument that the information is personal information.

In considering the complaint, however, the APC found that the publicly available character of the telephone directory information was a complicating factor. Under PIPEDA, consent to collect or use publicly available information is not required,[134] and telephone directory information is expressly considered to be publicly available information.[135] Because the respondent company sold subsets of directory information in response to requests for individuals who matched particular demographic profiles, the APC characterised the personal information at issue in this case as publicly available information, even though the contents of any given list were determined by selecting those names and addresses which matched the client's geodemographic parameters. According to the APC, assumptions that had been made about gender and ethnicity based on the names were simply that— assumptions. As for the sorting that took place based on geodemographic characteristics, the APC found that 'the fact that a person lives in a neighbourhood with certain characteristics'[136] was not personal information about that individual. The aggregate geodemographic information was considered to describe the neighbourhood rather than specific individuals.

It is not clear how the assumptions in this case are different from the inferences in the two cases discussed earlier involving the values associated with properties.[137] In those cases, the APC had found that the information that could be inferred from the values was personal information. While the purchase price of a house might permit one to infer that the purchaser was a good negotiator, this inference is not necessarily correct, and many other inferences are possible. In an environment where information that permits inferences about individuals can be personal information, it becomes important to identify the point at which inferences shift from educated guesses to personal information.

[133] *Lawson v Accusearch Inc* 2007 FC 125 (Federal Court, Ottawa). In *Johnson v Bell Canada* 2008 FC 1086 (Federal Court, Ottawa) Zinn J ruled that email communications about an individual were that person's personal information regardless of their contents.

[134] PIPEDA (n 29) ss 7(1)(d), 7(2)(c1) and 7(3).

[135] *Regulations Specifying Publicly Available Information*, SOR/2001–7.

[136] PIPEDA Case Summary #2009–004, 'No Consent Required for Using Publicly Available Personal Information Matched with Geographically Specific Demographic Statistics' <http://www.priv.gc.ca/cf-dc/2009/2009_004_0109_e.cfm> accessed 27 November 2010.

[137] Case Summary #2009–002 (n 75); Case Summary #2008–390 (n 127).

The case of crime maps also highlights the challenges of inferences based upon information in a geographic context. Crime maps published by police services typically map information about crime incidents that is otherwise publicly accessible—although not on the same scale, with the same ease, or with the same visual impact.[138] The information in the maps can be used in a variety of ways. Companies selling security services or alarm systems might identify neighbourhoods where there has been a rash of burglaries and might then mail information about their products or services to the residents of that neighbourhood. In this way, information about crime is associated with a sector of the city, which is in turn associated with the individuals who live in that area. Insurance companies could also use this information to raise the premiums of customers living in particular areas.[139] The question is: is this information about crime in the neighbourhood personal information once it is associated with individuals living in that neighbourhood? It is difficult to see why, for public policy purposes, it should be considered to be so. Like the case of the flood plain, the information is personal only by inference. Perhaps the key to these examples is that where one lives is 'public' information and observations about one's community do not become the personal information of each resident because it is not sufficiently personal. Yet if this is the key, then the decision in the CIPPIC complaint is hard to reconcile. While the aggregate geodemographic data may have been 'about' the community, it revealed information not readily observable, and it was linked to specific individuals about whom other personal inferences had been drawn. The objective was to profile individuals and not just to profile neighbourhoods in which individuals might live.

A final illustration of the difficulties with assumptions linked to geographical information associated with individuals comes from a news story reported in 2008.[140] According to this report, an individual applied to a Canadian bank for a loan to purchase a vehicle. The individual had a good credit rating, but was refused the loan. Unable to understand the refusal, he engaged the help of the media. A bank employee told a reporter, in a recorded conversation, that the bank had issued a list of postal codes to bank employees and instructed them to refuse credit to all individuals sharing the postal codes. The listed codes included all First Nations reservations in Canada, and the individual who had been refused a loan happened to live on a reservation.While this case raises issues of discrimination, it is also interesting to consider whether the assumptions made by the bank about individuals living at the specific postal codes became the loan applicant's personal information

[138] For a Canadian example of such a crime map see: Ottawa Crime (n 4).

[139] Julie Wartell and J Thomas McEwen, *Privacy in the Information Age: A Guide for Sharing Crime Maps and Spatial Data* (US Department of Justice, July 2001) 6, 18–19. Wartell and McEwen note that the raising of insurance rates is a risk frequently associated with crime mapping. However, they also note that insurance companies already use crime data associated with ZIP codes, and that there is no evidence to link actual crime maps with decision-making related to insurance rates.

[140] CBC News, 'Laurentian Bank loan blacklist targets aboriginal reserves' (Ottawa, 26 September 2008) <http://www.cbc.ca/canada/ottawa/story/2008/09/26/ot-loan-080926.html> accessed 3 January 2011.

when it was determined that he shared the characteristics that made him unattractive to the bank as a customer. If it is personal information, then the bank may have used it without the applicant's knowledge or consent, in contravention of PIPEDA.

These questions are crucially important in the context of GIS and information maps. Certainly, in some of the cases discussed above, the broader public policy issues may include consumer protection and discrimination—although a compelling data protection argument remains.[141] As GIS place certain information in a geographic context, and as individuals may also be linked to particular locations, there is the potential for details about the geographic context of identifiable individuals to be revealed. The challenge is to find the line beyond which this information becomes 'personal information'.

D Conclusions

Although personal information tends to be defined in Canadian data protection statutes as 'information about an identifiable individual', the case law has yet to reach a clear consensus on the standard for assessing when information is personal information. It suggests that some information linked to individuals is *about* them, while some is not. Yet the distinctions between the two kinds of information are sometimes difficult to draw. The situation is made more complicated when information permits inferences to be drawn about individuals. Decision-makers must be conscious of the distinction between actual and inferred information and may need to develop concrete guidance as to which inferences trigger data protection concerns and which are more properly the domain of other public policy measures.

The 'identifiable individual' also raises challenges with respect to information in a geographical context. There appear to be two competing tests at present in Canadian data protection law. The *Pascoe* test of a 'reasonable expectation' that an individual may be identified is well established in Ontario, and courts and adjudicators in other provinces have adopted this test. At the federal level, a competing 'serious possibility' of identification standard has emerged, and it is not clear to what extent this test is different from that in *Pascoe*. Neither test may be well suited to dealing with the proliferation of computerised data that is becoming available through a growing range of sources, and that may permit the re-identification of individuals in previously de-identified data sets, or that may alter, from one day to the next, the 'reasonable expectation' or the 'serious possibility' that individuals can be re-identified.

[141] Patricia Kosseim and Khaled El Emam, 'Privacy Interests in Prescription Data, Part I' (January–February 2009) 7(1) IEEE Security and Privacy 72 argue that there are other public policy objectives besides physician privacy that are served by preventing the mining of this information by those who engage in direct marketing to physicians—including reducing the costs of the health care system. One should perhaps be careful not to ask data protection law to carry the weight of other public policy objectives. See also Kosseim and El Emam, 'Privacy Interests in Prescription Data, Part II' (n 94).