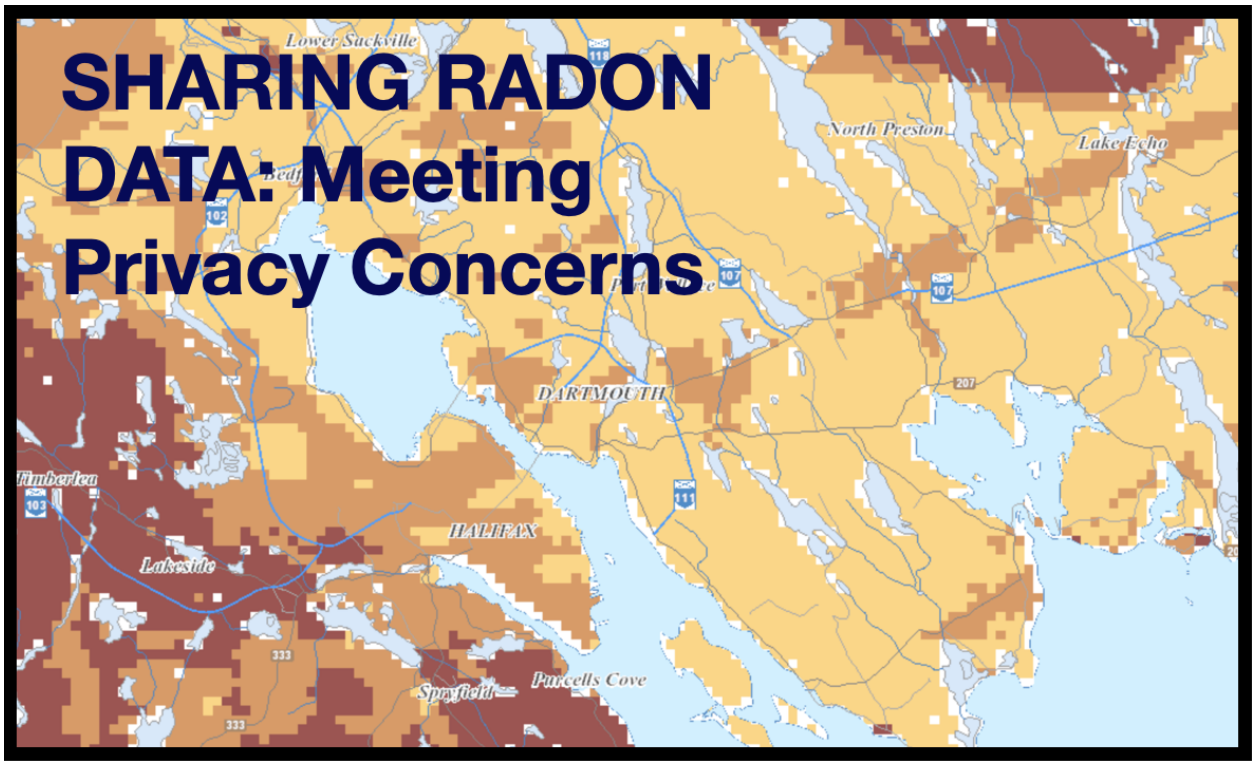
BC LUNG FOUNDATION



Sharing Radon Data: Meeting Privacy Concerns
Healthy Indoor Environments, Legal Brief No. 10

Author: Noah Quastel LLB LLM PhD
Director, Law and Policy,
Health Indoor Environments,
British Columbia Lung Foundation

Revised November 16, 2021

This project was made possible by funding from:

THE LAW FOUNDATION OF BRITISH COLUMBIA

real estate foundation BRITISH COLUMBIA

Summary

Radon gas is a naturally occurring radioactive gas, emanating from the ground and often entering and remaining in buildings. Radon exposure is the leading cause of lung cancer after smoking. Whether radon levels indoors exceed the Government of Canada's Radon Guideline of 200 Bq/m^3 depends on a mix of building characteristics and underlying geological and soil conditions. Good radon databases and maps are important not only for academic researchers, but policy makers designing radon policy, homeowners who want to know their local risks, and various professionals, including architects, engineers, builders, employers, rental property managers and real estate agents, who play a role in ensuring buildings and indoor spaces are safe.

Many organizations collect radon data, including academic researchers, citizen science projects, lung health nonprofits and private sector radon labs. However, database managers and mappers face challenges in finding radon data in part because some organizations are fearful about sharing radon data due to privacy concerns. This brief canvasses the law of privacy in Canada to help offset these concerns. It discusses whether radon data should be understood as personal information, and any potential legal limits on sharing data. It provides a clear roadmap for how data can be shared.

This brief argues that radon data about specific properties are not 'personal information' and so not protected by Canadian privacy law. However, organizations that are still worried-- if, for interest they want to ensure broader privacy values are respected-- there are clear steps they can take that still allow radon data to be shared with databases and maps. This brief discusses the role of consent forms, anonymization techniques in database files and maps, and data sharing agreements.

Acknowledgements

The author would like to thank the close involvement of members of the Canadian Radon Database and Mapping Working Group for help formulating questions and reviewing contents of this report. Members include:

John Drage, Geosciences and Mines Branch, Government of Nova Scotia

Jean-Philippe Drolet, Institut National de la Recherche Scientifique

Michel Gauthier, Health Canada

Colin Gutcher, Health Canada

Brad Harvey, Geological Survey of Canada

Jeffrey Trieu, British Columbia Centre for Disease Control

Anne-Marie Nicol, Simon Fraser University

Noah Quastel, British Columbia Lung Foundation

Pam Warkentin, Canadian National Radon Proficiency Program and Canadian Association of Radon Scientists and Technologists

More information on the Canadian Radon Database and Mapping Working Group is available at https://bclung.ca/programs-initiatives/healthy-indoor-environments-program/current-projects/radon-mapping-working

About Our Organization

The BC Lung Foundations's Healthy Indoor Environments program is focused on providing education, resources, and policy options for addressing priority indoor air pollutants in British Columbia. Canadians spend 90% of their day indoors, with about 70% at home and 20% at work or school. The air we breathe indoors can contain particulates, gases, allergens and fumes that can significantly impact our health in both the short and long term. Knowing the main indoor air pollutants, their sources, and how to reduce them are key to reducing harm to our health. For more information visit our website at https://bclung.ca/programs-initiatives/healthy-indoor-environments-program

Table of Contents

1. Introduction

Many organizations hold extensive data on radon test results for particular homes and buildings, allowing results to be linked to specific addresses or Global Positioning System (GPS) coordinates. Examples of such entities include radon device companies with laboratories, but might also include non-profits which promote radon testing, such as a provincial lung foundation. (For short, I will simply use "organizations"). Organizations' data could potentially be used to provide to the public databases and detailed radon maps. Databases can be helpful for radon research, and to establish what locations have high radon potential. Radon maps could help people know readings in their area and encourage them to test and mitigate for radon. However, some organizations may resist sharing data, or not have received consent to share information supplied by clients. Radon test data, like many new technologies that disclose individual environmental information, can thus involve a complex set of tradeoffs between improving knowledge and standards, and potential abuses of personal privacy.[1] Fears include profiling and data mining of information on consumer behaviours; exploitation for direct marketing purposes[2] or simply public awareness and associated shame of the radon level attached to a home.

We have written this Legal Briefing Note because we found widespread fear among organizations, radon scientists, and mappers about violating privacy law. Some organizations have been reluctant to release radon data and some scientists have suggested they might need to create relatively unrefined maps, using statistical averages across large areas.[3] We do not want unjustified fears to create obstacles to good maps being created.

This Briefing Note concerns the specificity of information that organizations and mapping agencies can release in Canada and draws on Canadian federal, territorial and provincial law. We did review academic articles on Canadian privacy law, statutes, and decisions by privacy commissioners and courts. As well, we have interviewed data scientists, radon experts, and radon testing organizations. We have chosen not to cover privacy law issues outside of Canada, although increasingly companies with international reach also seek to comply with strict standards such as the European Union's *General Data Protection Regulation* and the *California Consumer Privacy Act*. As well, this brief does not focus on radon testing conducted on behalf of government (such as for public buildings) or radon testing of businesses compelled by licensing or permitting requirements.

---

[1] Kuh, K. 2012.Personal Environmental Information: The Promise and Perils of the Emerging Capacity to Identify Individual Environmental Harms. Vanderbilt Law Review 65 (6), 1566; Keßler, C. and McKenzie, G., 2018. A geoprivacy manifesto. Transactions in GIS, 22(1), pp.3-19.

[2] Kalkbrenner, A. and Unger, J., 2018. Energy consumption data and rights to privacy: climate change mitigation policy, privacy and the "internet of things" in Alberta. Environmental Law Centre (Alberta).

[3] In researching this paper for instance, we encountered companies which did not want to release data at all, and scientists that thought the most refined maps they could legitimately produce generalized across Canadian "forward sortation areas"— the first 3 digits of the postal code, and which in some areas of Canada can cover hundreds of square kilometres.

2. Main Findings

It is doubtful that release of radon readings could violate privacy law. Many people do feel strongly that there is something private about the radon levels in a home. However, in order for radon test results to be covered by privacy law they need to count as 'personal information' under the definitions in statute. While the issue of radon readings and privacy has not been considered by any court or tribunal we could find (in Canada), our review of decisions by privacy commissioners and courts across Canada suggest it is unlikely that legal decision-makers will conclude that radon test results linked to postal address are legally personal information. This should be enough to dispose of the issue. However, we cannot rule out the (remote) possibility that courts might rule that radon data is personal information. We have thus done further analysis of what organizations should consider under the alternative option that radon data linked to address is treated as personal information. Organizations might also pursue these routes to capture the non-legal but broader ethical sensibility (of many but not all people) that radon data linked to home address should be protected.

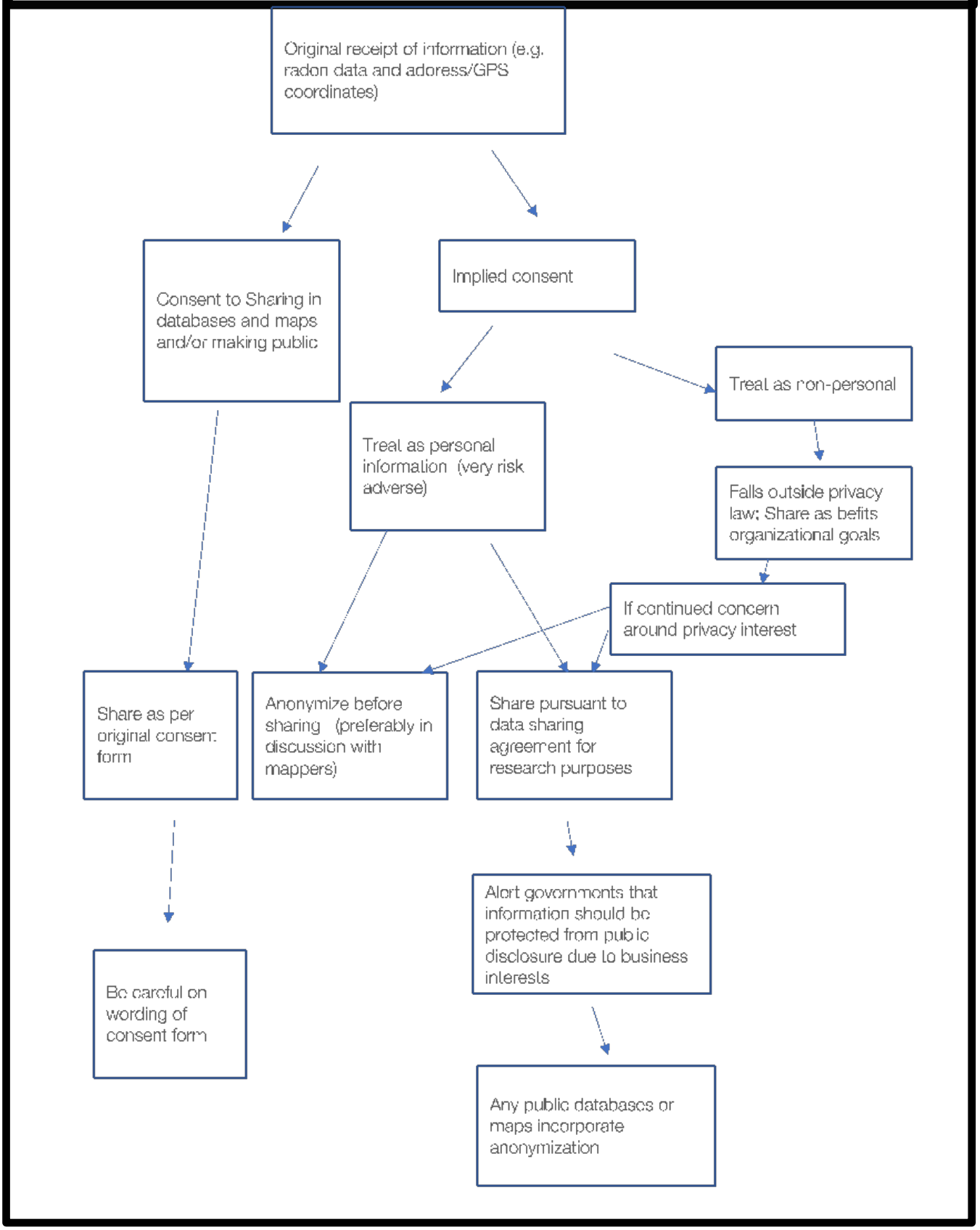
Under the alternative option that privacy principles remain important, there are acceptable ways for organizations to hold and release radon readings to database managers and mappers. Privacy laws generally do allow organizations to collect personal information. If homeowners seek to know radon readings and contract with organizations to learn this, the collection of radon data will be deemed part of the service, and consent will be implied. An organization can share information in three ways. First, consent to share can be obtained at the beginning of the process. Second, data can be anonymized—stripped of any identifying information-- before it is shared. Third, there are also legislative provisions that provide a procedure for an organization to release personal information to researchers. In order to do so, it is necessary that the research requires precise data, and there need to be guidelines in place for the removal or destruction of individual identifiers at the earliest reasonable time. Data sharing agreements can include provisions that only anonymized data will be made public.

A host of techniques are available to mappers to create sufficiently precise maps that anonymize data. For radon data, there are easy techniques for obscuring or changing locations so that data no longer identifies particular addresses. In this Brief we describe the laws on de-identification and relevant anonymization techniques that still allowing mappers to produce refined and useful maps. In situations where organizations choose to be very risk adverse, they may pre-anonymize data (and so strip it of in any way being personal information) before disclosing it to outside organizations.

Organizations should not be fearful that government owned and person-identifying datasets will be made public through Freedom of Information requests. Some organizations are fearful that once data is in the hands of a public agency, Freedom of Information laws come into play such that a request for information could result in data being released. Beyond protections for privacy of personal information, freedom of Information legislation also provides for exceptions for the release of third-party information where information is supplied in confidence and releasing it might

harm business interests. Organizations can explicitly cite privacy and business interests and expectations of confidentiality in data sharing agreements. Freedom of information does allow, at times, for overrides of protections for personal privacy and third-party business interests when health and safety is at stake or, in some cases, where there are pressing public interest values involved. However, it is extremely unlike that these provisions would be successfully invoked in ways that would result in radon data linked to address being publicly released. Where there are compelling or urgent health and safety considerations (e.g. in the very rare cases of exceptionally high radon readings), public bodies will almost always be able to notify occupants rather than have a broad public disclosure. There is likely a public interest in knowing community level radon readings, but these can be accomplished through releasing anonymized radon data.

Decision Process for Sharing Radon Data



Organizations should be mindful around obtaining consent. Some organizations do not now ask for consent, relying as it were on the implicit consent provisions of privacy law. This is alright, given that obtaining name and address of clients is a normal part of doing business (and so allowing for geo-coding of radon data). However, some organizations have poorly worded consent forms that promise never to share data. This creates a contractual obligation that bars data sharing far stricter than anything required by privacy law. Organizations should have a plan for how they will use data from the point of collection to final distribution (e.g. including sharing with database managers and mappers) and either ensure that complies with implicit consent processes, or, alternatively word formal consent process in a way that ensures data can be shared down the road. In the section on 'obtaining consent' we suggest important clauses to be put into consent forms.

3. Relevant Statutes

In Canada, privacy protection is spread across a number of different federal and provincial statutes, and the result is at first blush confusing. This is necessary, however, to properly ensure coverage:

(a) **The private sector that falls under federal jurisdiction** (*Personal Information Protection and Electronic Documents Act* --PIPEDA).[4] PIPEDA allows, but puts significant limits on how and when, organizations can collect and share personal information. Generally, organizations can collect information so long as persons' consent, but have significant limits on how they can share that information.

(b) **The federal public sector.** The *Privacy Act* provides that government agencies can collect personal information in some circumstances, and in turn citizens' have a right to information collected about them: As well, personal information is exempt from disclosure except under limited circumstances.[5] The *Access to Information Act* gives people the right to access records of government institutions. It provides a long list of exemptions, such as in cases of personal information, and confidential business information.[6]

The private sector falling under provincial jurisdiction. Here there are some complications due to overlap between federal and provincial jurisdiction. All businesses that operate in Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation). Organizations in the Northwest Territories, Yukon and Nunavut are considered federally regulated, and are therefore also covered by PIPEDA.[7] PIPEDA

[4] Personal Information Protection and Electronic Documents Act, SC 2000, c 5
[5] Privacy Act, RSC 1985, c P-21
[6] Access to Information Act, RSC 1985, c A-1
[7] Officer of the Privacy Commissioner of Canada, 2019. PIPEDA in Brief, available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/ accessed March 30, 2021

is thus, in practice, the default legislation. However, three provinces, British Columbia, Alberta, and Quebec have specific private sector legislation, which is deemed substantially similar to PIPEDA, and by agreement these apply to private sector organizations in those provinces. Where such legislation exists, private sector organizations are restricted in the collection of personal information, with a range of exceptions. Individuals can access information collected on them and request that any errors be corrected.[8] Other provinces have specific legislation for privacy over health records as well (which are not covered here).

The provincial public sector (for example, in in British Columbia, *the Freedom of Information and Protection of Privacy Act* (FIPPA)). This legislation a balances citizen's rights to freedom of information and open government with privacy concerns; while the general rule is a right to information, personal information is exempt from disclosure, except under limited circumstances. [9]

Radon data mapping will involve both public sector and private sector privacy law: Organizations will be concerned with what they legitimately collect and release to other entities (including public agency mappers); governments will be considered about what data they can store and release to the public, and organizations and governments will be concerned about when data held by government agencies might be subject to freedom of information requests and public interest disclosures.

4. Obtaining Consent

Privacy law generally puts limits on the degree to which organizations are allowed to collect personal information. Likewise, organizations can collect personal information if consent is obtained. This can also extend to sharing information with other organizations—e.g. if there is explicit description of the purposes for which sharing will occur. Governments can, generally, collect personal information in the normal course of programs and activities, either directly from the person or if the person has consented to another organization passing on the information but has strict limits on the use and disclosure of that information.[10]

In practice in Canada, organizations typically receive personal information in the normal course of doing business. Canadian privacy laws generally allow that consent will be implied if the purpose of collecting person information is obvious (e.g. as part of

[8] Personal Information Protection Act, SBC 2003, c. 63, Alberta, Personal Information Protection Act, c. P-6.5, s. 1(1)(k); Quebec—Act Respecting the Protection of Personal Information in the Private Sector, CQLR, P -39.1 s. 2

[9], Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165, Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25; The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01; The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31; Act respecting Access to documents held by public bodies and the Protection of personal information SQ A-2.1 Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6 ; Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 ,; Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5,; Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01; Access to Information and Protection of Privacy Act, RSY 2002, c 1; Access to Information and Protection of Privacy Act, SNWT 1994, c 20; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20,

[10] See, for example, Privacy Act, 1985, c P-21 s. 4 to 8

providing a service) and the individual provides the information[11] or if notice is given and a timeline for opting out provided.[12] Federal law (PIPEDA) allows for implied consent through use of a service[13], but emphasizes that "An organization should generally seek express consent when the information is likely to be considered sensitive" [14]

Organizations that collect radon readings—such as nonprofit lung foundations or radon laboratories—should be careful in how they script the consent process. Attention should be given, at the outset, on how data will be used. We have talked to organizations who found themselves restricted in their ability to share data because they provided consent forms which promised not to share data. Organizations that want to share data with researchers and for mapping purposes without running afoul of privacy law have a number of options.

i. The first is to rely on the implicit consent provisions, which can also be met by general statements such as "All data will be collected in conformity with privacy laws applicable in your province or territory". Whether or not radon data is seen as personal information (discussed further below), there are legitimate ways to share it without asking for consent. However, risk adverse organizations may instead pursue the next two options.

ii. Another option is to broadly describe potential future uses for the data, such as sharing with public sector databases and mappers. If an organization thinks its customers will approve, it can seek wide leeway to share and publicize radon information.

iii. A third option, which we think is the better approach, is to seek consent, but alongside detailing specific potential future uses of the information. For instance, the consent form could specify that

- radon data will be shared on a confidential basis with academic and other qualified researchers, government agency databases and mapping entities, subject to data sharing agreements, so as to better understand radon and its prevalence at the community level

- To the degree permitted by law, databases and maps available to the public would not link radon readings to an address or specific GPS coordinate

Sample language for such a provision is provided in Appendix B.

---

[11] Personal Information Protection Act, SBC 2003, c. 63 s. 8 (1); Personal Information Protection Act, RSA c. P-6.5,)s. 8(2); Act Respecting the Protection of Personal Information in the Private Sector, CQLR, P -39.1, s. 8 and 9; for other provinces and territories see Personal Information Protection and Electronic Documents Act, SC 2000, c 5 Schedule 1, 4.38

[12] PIPA, s. 8(3)(2); Alberta, PIPA s. 8(3)

[13] PIPEDA, Schedule 1, 4.3.8

[14] PIPEDA, Schedule 1, s. 4.3.6

We expect that organizations may differ concerning how to make the trade-off between clients' interest in safeguarding information and contributing to public knowledge. We suggest this option as a possible way of reconciling these competing values.

5. Is Radon Data "Personal Information"?

Privacy laws generally pertain only to "personal information". The first question to ask is whether the information at issue amounts to 'personal information'. A government body, for instance, could take steps outside of privacy and freedom of information law to release non-personal information.[15]

The majority of database custodians and radon professionals we talked to assumed that radon test results were "personal information" and so covered by these laws. At times this was a mere assumption, and at times the reasoning was that a radon test result could make a difference to the value of a home, and potentially change sale price. Some organizations simply voiced concern about the expectations and desires of their clients. However, legal decisions in Canada suggest that for legal purposes, radon data on properties is not personal information.

The various acts define personal information. For the most part, the definitions are very open ended. For instance, PIPEDA defines "personal information" as "information about an identifiable individual".[16] Some statutes provide a more precise list that might include a person's address or medical history.[17]

Various legal sources for interpreting these clauses include decisions of Privacy Commissioners, court cases, and Interpretive Bulletins.[18] Privacy law involves different statutes and the general legal principle applies that each statute is to be interpreted independently. However, two trends work to create greater consistency than might at first blush appear. First, the courts will strive to render consistent the meaning of terms that appear in statutes of the same legislature. Alberta courts have thus reasoned that the use of 'personal information' in public freedom of information statutes was much the same as

---

[15] Ministry of Water, Land and Air Protection, Re, 2001 CanLII 21606 (BC IPC) ("Order 01-52") para. 76.

[16] PIPEDA, s. 2(1); See also British Columbia, Personal Information Protection Act, SBC 2003, c. 63, s. 1(1); Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165, Schedule 1; Alberta, Personal Information Protection Act, c. P-6.5, s. 1(1)(k); Quebec—Act Respecting the Protection of Personal Information in the Private Sector, P -39.1 s. 2

[17] Privacy Act, RSC 1985, c P-21 section 3; Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25, s 1 (n)(1); The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s. 24(1); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 3; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6 s. 1; Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 , s. 2(u); Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5, s. 3(1)(i); Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01,s.1(i); Access to Information and Protection of Privacy Act, RSY 2002, c 1 s. 3; Access to Information and Protection of Privacy Act, SNWT 1994, c 20 s. 2; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20, s. 2

[18] Office of the Privacy Commissioner, 2013. Interpretive Bulletin. Personal Information. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

in private sector personal information protection statutes.[19] Second, our review of decisions across Canadian courts and privacy officer decision-making shows considerable borrowing from other jurisdictions and attempts to harmonize reasoning.

The general rule is that to qualify as personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed.[20] Accordingly, information about residential properties does count as personal information when it is linked to particular persons. For instance, residential property appraisal documents constitute the personal information of the property owner, including the selling/purchase price of an individual's home.[21]

However, a number of cases hold that details about buildings (such as, inter alia, market value, assessed value, date of construction, insulation type, and basement height) do not count as personal information when the property owner or occupier's name is not attached. In a relatively early decision under *Ontario's Freedom of Information and Protection of Privacy Act, 1987* Commissioner Sidney Linden made a distinction between information that qualifies as "personal information" and information about residential properties:

> The owner of a property may or may not be an individual, and individual property owners, may or may not reside in the property they own. In many cases an individual's address may have nothing whatsoever to do with property ownership, as is the case with the large proportion of properties occupied by tenants. It is clear to me that the municipal location of a property cannot automatically be equated with the address of its owner, notwithstanding that many individuals do reside in the properties they own…
>
> In considering whether or not particular information qualifies as "personal information" I must also consider the introductory wording of subsection 2(1) of the Act, which defines "personal information" as "...any recorded information about an identifiable individual...". In my view, the operative word in this definition is "about". The Concise Oxford Dictionary defines "about" as "in connection with or on the subject of". Is the information in question, i.e. the municipal location of a property and its estimated market value, about an identifiable individual? In my view, the answer is "no"; the information is about a property and not about an identifiable individual.[22]

Many decisions since then have allowed information about residential properties to be disclosed on the grounds that it was not personal information.[23] This includes information about properties for which building permits were sought,[24] which were considered as possible landfill sites,[25] which were tested for water quality,[26] tested for indoor air quality in

---

[19]Edmonton (City) v Alberta (Information and Privacy Commissioner), 2016 ABCA 110 para. 23-24
[20] Ontario (Attorney General) v. Pascoe, 2002 CanLII 30891 (ON CA)
[21] Office of the Privacy Commissioner, 2008. Residential Property Appraisal Documents are Owners' Personal Information: PIPEDA Case Summary #2008-390. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2008/pipeda-2008-390/ accessed August 8, 2019
[22] Information and Privacy Commissioner Ontario Order 23, dated October 21, 1988, cited in Toronto (City) (Re), 2007 CanLII 8396 (ON IPC) "Order MO-2153"
[23]Ontario (Finance) (Re), 1996 CanLII 7407 (ON IPC); Toronto (Property Assessment Corporation) (Re), 2006 CanLII 50683 (ON IPC)
[24] Whitchurch-Stouffville (Town) (Re), 1993 CanLII 4957 (ON IPC) ("Order M-138")
[25] Metropolitan Toronto (Municipality) (Re), 1993 CanLII 5007 (ON IPC) ("Order M-188")
[26] Ontario (Transportation) (Re), 2004 CanLII 56440 (ON IPC) ("Order PO-2322")

relation to trichloroethylene pollution and identified using GPS coordinates[27], and with arrears of municipal taxes.[28] One decision found that tests of well water accompanied with legal land descriptions were not personal information.[29] In one Ontario case, an extensive database on properties could be released (including market value, assessed value, year of construction, number of bedrooms and bathroom, insulation type, floor areas, etc.) once the property owner or occupier's name was unattached.[30] The Alberta Court of Appeal notes that "Information that relates to an object or property does not become information 'about' an individual, just because some individual may own or use that property."[31]

There are no decisions that directly address the issue of radon test results. While we think it is very likely that courts and tribunals would treat radon like other information about property, there are two caveats that make it difficult to have absolute certainty.

First, in some cases commissioners and courts have found it difficult to draw clean lines around what counts as personal information and not, allowing that some property information can have a 'personal dimension."[32] Drawing the dividing line thus requires consideration of the context in which information appears.[33] There is evidence that some people who discover that their homes have high radon levels face significant worry, guilt and stigma.[34] It cannot be ruled out that a privacy commissioner would feel it falls into personal information.

A second issue concerns data linkage. Since earlier privacy decisions (e.g. in the 1990s) there has been a significant growth of computer based and internet accessible data, giving rise to concerns over data being linked with other data. More recent decisions have thus incorporated the reality that even if an individual is not specifically named in a record, the context in which information is given, its nature, content and other factors may mean that an individual is identifiable, thus making the information 'personal information'.[35] The proper test is whether it is reasonable to expect that, when information is combined with information from sources otherwise available, an individual can be identified.[36] It is now common to refer to locational information as a "quasi-identifier"—for instance given

---

[27] Ontario (Environment) (Re), 2009 CanLII 10052 (ON IPC)("Order PO-2763")
[28] St. John's (City) (Re), 2017 CanLII 2264 (NL IPC)
[29] Alberta Health (Re), 2012 CanLII 70607 (AB OIPC)
[30] Toronto (Property Assessment Corporation) (Re), 2006 CanLII 50683 "Order MO-2030"
[31] Leon's Furniture Ltd. v Alberta (Information and Privacy Commissioner), 2011 ABCA 94. at para. 48.
[32] Edmonton (City) v Alberta (Information and Privacy Commissioner),2016 ABCA 110 (CanLII) at para 25
[33] Alberta Health Services (Re), 2018 CanLII 7268 (AB OIPC) "Order F2018-09" at para 17
[34] This is extensively documented in Edelstein, M.R. and Makofske, W.J., 1998. Radon's deadly daughters: science, environmental policy, and the politics of risk. Rowman & Littlefield.
[35] Edmonton (City) v Alberta (Information and Privacy Commissioner), 2016 ABCA 110 (CanLII), Toronto Catholic District School Board (Re), 2019 CanLII 17538 ("Interim Order MO-3736-I"); Ontario (Community Safety and Correctional Services) (Re), 2014 CanLII 73024 (ON IPC) ("Order PO-3429, Appeal PA09-107A")
[36] Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner),2001), 2001 CanLII 32755 (ON SCDC), Ontario (Attorney General) v. Pascoe, 2002 CanLII 30891 (ON CA) see also Office of the Information and Privacy Commissioner of Ontario in Order PO-2811, [2009] O.I.P.C. No. 127, upheld in in Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner), 2012 ONCA 393 (CanLII); Schindler Elevator Corporation (Re), 2012 BCIPC 25 ("Order P12-01")

the address of a doctor's office it is likely that a person could find out the name of the doctor.[37]

For these reasons, a very risk adverse organization may prefer to treat radon data as having a protected status within privacy law (or on solely ethical and reputational grounds). They may then proceed to release information in one of two ways (in the event that there is no prior consent to sharing with databases). First, data can be delivered pre-anonymized. In some cases, this need not significantly interfere with the quality of the information presented— some techniques for anonymization can still allow considerable precision in mapping radon test results. Second, organizations might release data pursuant to research sharing agreements, in which the agreements have specific protections in place, foremost of which the personal information is not released to the public. These two approaches will be discussed further below.

6. Permitted Non-Consensual Disclosure

There are a variety of circumstances in which privacy law allows personal information to be disclosed, without consent of the original provider, to another organization (such as a government database and mapping project).

In the normal case, personal information can be disclosed only if consent is obtained. However, private sector privacy laws provide limited circumstances in which non-consensual disclosure can happen.[38] The acts include a range of circumstances, including inter alia, medical treatment when consent not possible, or criminal investigations. The two areas we examine here include research purposes, and immediate harm.

a. Sharing for Research Purposes

Both private sector and public sector privacy statutes allow use and disclosure of identifying personal information without consent for research and archive purposes. [39]

---

[37] Emam, K. E., & Arbuckle, L. (2013). Anonymizing Health Data: Case Studies and Methods to Get You Started. Sebastopol, CA, USA: O'Reilly Media, Inc see especially Chapter 9. Geospatial Aggregation: Dissemination Areas and ZIP Codes

[38] PIPEDA, s. 7(3), Personal Information Protection Act, SBC 2003, c 63 s. 18, Personal Information Protection Act, SA 2003, c P-6.5, s.20; Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 s. 18

[39] PIPEDA, s. 7(3)(f); Privacy Act, 8 2 (j), Personal Information Protection Act, SBC 2003, c. 63, s. 21(1); Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 s. 22(4)(d) and s. 35,; Alberta, Personal Information Protection Act, c. P-6.5 s. 20(p); Personal Information Protection Act Regulation, Alta Reg 366/2003, s. 12 to 14; Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25, s. 14(j) and (k);,20(p) and (q) ; The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s. 29(2)(k); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175 s. 17(4)(d) and s. 47; Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 21(1)(e); Quebec—Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c. P-39.1, s. 18(8) and s. 21; Act respecting Access to documents held by public bodies and the Protection of personal information CQLR, c. A-2.1, s. 78; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6 46(1)(b.1) and 47.1,; Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 (s. 40(1)(e) and s. 70; Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5 s. 20(4), s. 29, and s. 30, ; Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s. 15(2)(d), s. 39, and s. 40; Access to Information and Protection of Privacy Act, RSY 2002, c 1, 25(3)(d) and s. 38 ; Access to Information and Protection of Privacy Act, SNWT 1994, c 20 s. 23(4)(d) and s. 49 ; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20, 23(4)(d) and s. 49 See also Ogbogu, U, and

While the exact terms vary, British Columbia's *Freedom of Information and Privacy Act* at s. 35 provides one delineation of necessary conditions:

- the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form
- the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in the research,
- any data linking is not harmful to the individuals that information is about and the benefits to be derived from the data linking are clearly in the public interest,
- guidelines are in place for the removal or destruction of individual identifiers at the earliest reasonable time;
- there is an agreement in place (these are often called 'research sharing agreements').

Further insight on this can be gleaned from decisions of the British Columbia Information and Privacy Commissioner. An information-sharing agreement sets out the terms and conditions for how the personal information will be collected, used, and disclosed by the entity receiving the data. Information-sharing agreements also enhance the transparency and accountability of public bodies with respect to data flows of personal information and how the privacy of individuals is being protected.[40] *FIPPA* Section 35 prescribes conditions that are designed to protect personal privacy, but it is important to recognize that it is intended to operate as a discretionary authority for disclosure. It provides a vehicle for authorizing access to information for research or statistical purposes, if the prescribed conditions are met. The Ministry's exercise of its discretion to not disclose data may be reviewed by the Commissioner under the residual review powers of *FIPPA*.[41]

Organizations should see these provisions as both allowing them to share data with radon database managers and mappers, and also ensuring that research sharing agreements will be in place. Organizations can insist, as part of research sharing agreements, that final, publicly accessible databases and maps not reveal (or allow clever analysts to link) radon readings with specific addresses or coordinates. These principles can be seen in the BC Centre for Disease Control's (BCCDC) data sharing agreement for the BC Radon Data Repository, an integrated provincial database of indoor radon measurement data (Appendix C). Below we discuss anonymization techniques that can be used by mappers to ensure these safeguards.

Burningham, S. 2014. Privacy Protection and Genetic Research: Where Does the Public Interest Lie?, 2014 CanLIIDocs 56 (Alberta Law Society Review).

[40] Electronic Health Information System (Re), 2010 BCIPC 13 (CanLII)) Investigation Report F10-02 at para 118

[41] British Columbia (Education) (Re), 2010 BCIPC 42 (CanLII

b. Immediate Harm

Private sector privacy laws allow organizations to release information without consent if pressing or compelling safety issues are at play.[42] For instance, PIPEDA s. 7(3)(e) provides that an organization *may* disclose personal information without the knowledge or consent of the individual only if the disclosure is, among a number of reasons, "made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure". While specific language shifts between different legislation, the provisions are similar in that there is an exemption from privacy law considerations for emergency situations. We did not find cases under private sector privacy legislation. As we will discuss further, below, there are many examples of this being adjudicated under public sector legislation and similar reasoning will likely apply. The bar is quite high, requiring a significant, emergency like circumstance. Similar principles likely apply to the private sector.

In rare occasions of extremely high radon readings, specific radon data (at e.g. GPS coordinate or address level) would be captured by these provisions. In these cases there are moral reasons for disclosing information, not only, e.g. by sending test results to the person as part of the normal process for radon tests, but also contacting local health authorities. However, in most cases of elevated radon, the case for urgency will not be made out. In a later section we discuss how emergency safety issues play out in public sector privacy law.

7. De-identification

In Canadian privacy legislation, personal information must uniquely identify a person. Once information is rendered anonymous, it ceases to be 'personal'.[43] The person from whom the information was originally obtained can then no longer claim a

---

[42] PIPEDA, s. 7(3)(e); Access to Information Act, RSC 1985, c A-1 s. 20(6)(a), Personal Information Protection Act, SBC 2003, c. 63, s. 15(1)(l), Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 s. 22(4)(b) ,; Alberta, Personal Information Protection Act, c. P-6.5, s. 20(i); Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25 s. 32(1)(a); The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s 29(2)(m); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; s. 17(4)(b) Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 42(1)(h); Act respecting the protection of personal information in the private sector, CQLR c P-39.1 s. 18(7); Act respecting Access to documents held by public bodies and the Protection of personal information CQLR, c. A-2.1 59(4),; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6,s.33.1; Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 s. 9(3); Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5 s. 20(4)(b),31(1)(a) ; Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s. 30; Access to Information and Protection of Privacy Act, RSY 2002, c 1,; Access to Information and Protection of Privacy Act, SNWT 1994, c 20; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20

[43] Kosseim, P. and Brady, M. 2008. Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes. McGill Journal of Law and Health.2008 CanLIIDocs 5

privacy interest in it.[44] As such "de-identification to protect privacy continues to be an acceptable and reasonable process of protecting privacy".[45]

As well, where there are provisions for data sharing for research purposes, efforts must be taken to de-identify when possible, and at the earliest possible opportunity. As noted above, de-identification must also take into account potential data linkages: The proper test is whether it is reasonable to expect that, when information is combined with information from sources otherwise available, an individual can be identified.[46]

In many contexts there are standardized procedures for de-identification. For instance, United States Health law provides that health entities (such as hospitals) can use and disclose de-identified information.[47] Entities that want clarity can use "Safe Harbour Rules". These provide that for geographical information, precise information should only be provided to the provision of the first three digits of a ZIP Code if it contains more than 20,000 people.[48] Some Canadian radon experts followed a similar approach, suggesting to us that geographical information be limited to Canadian Forward Sorting Areas (e.g. as defined by the first three digits of a postal code). However, experts in geographical information systems have been able to offer more sophisticated approaches. It is worth setting this out.

Cropping. ZIP and postal codes are typically seen as too small to protect anonymity. "Cropping" refers to retaining only the first *x* number of characters. For example, the Canadian postal code "K1L8H1" could be cropped to its three-character

---

[44] An early United Kingdom case establishing this is R. v. Department of Health, Ex arte Source Informatics Ltd., [2001] QB 424, [2000] 1 All E.R. 786, 2 WLR 940.

[45] Ronald J. Kruzeniski, Q.C,. Saskatchewan Information and Privacy Commissioner in Saskatchewan Health Authority (Re), 2019 CanLII 44080 (SK IPC) at para. 19; see also Kosseim and Brady ibid, Information and Privacy Commissioner of Ontario, 2016. De-identification Guidelines for Structured Data. Available at https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf accessed July 13, 2020

[46] Ontario (Attorney General) v. Ontario (Information and Privacy Commissioner),2001), 2001 CanLII 32755 (ON SCDC), Ontario (Attorney General) v. Pascoe, 2002 CanLII 30891 (ON CA) see also Office of the Information and Privacy Commissioner of Ontario in Order PO-2811, [2009] O.I.P.C. No. 127, upheld in Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner), 2012 ONCA 393 (CanLII); Schindler Elevator Corporation (Re), 2012 BCIPC 25 "Order P12-01"

[47] Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, section 164.514.

[48]For more explanation see US Department of Health Services, 2012. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. available at https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

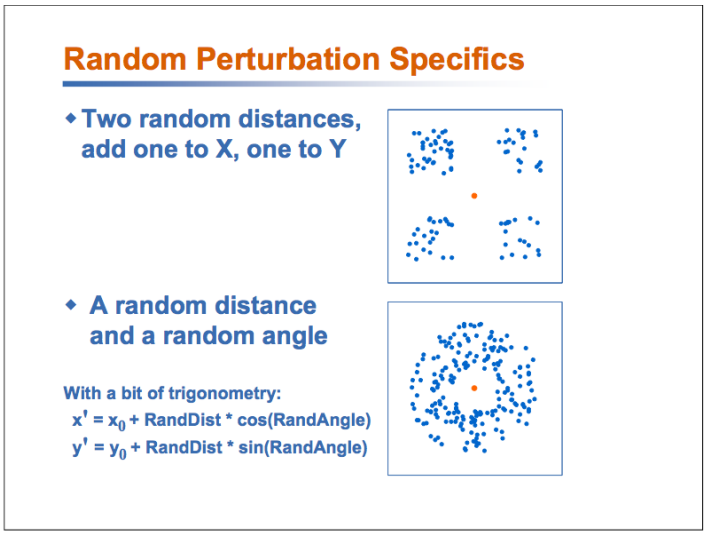


Figure 1: Random Perturbation. from Stinchcomb, D. 2004. Procedures for Geomasking to Protect Patient Confidentiality. ESRI international Health GIS Conference October 19, 2004.

version "K1L". However, the cropped area may be so large that any local information is lost. Moreover, more refined techniques may still protect anonymity.[49]

Clustering. Here, adjacent areas are grouped into larger ones. The advantage of clustering over cropping is that we can get much smaller areas while ensuring that the risk of re-identification is below threshold. Details on how to cluster are provided in Emam and Arbuckle's *Anonymizing Health Data: Case Studies and Methods to Get You Started*.[50]

Obfuscating. One radon testing company told us that they often "obfuscate" data: While they have street level address information, coupled with the latitude and longitudes for the address, they supply mapping agencies with the information blurred to the latitude or longitude minute. This creates an area of roughly 1.8 km x 1.8 km. In some remote areas this may still identify individual properties.

Random perturbations or "jittering". Obfuscating is only one of a number of growingly sophisticated methods for "geomasking" data. Mappers are increasingly making use of Geographical Information System software that allows data points to be offset to hide precise locations. For instance, for a precise point, a new point can be generated close by, with the precise distance and angle randomly generated so that viewers cannot reconstruct the process to find specific locations. Moreover, this process can be adjusted to balance the need for geographical specificity with anonymity. In denser urban areas, the distances can be smaller. To do this, mappers can calculate the distance the information is offset as a function of population density. This allows for maps that preserve locational

[49] Armstrong, M.P., Rushton, G. and Zimmerman, D.L., 1999. Geographically masking health data to preserve confidentiality. Statistics in medicine, 18(5), pp.497-525.
[50] Emam, K. E., & Arbuckle, L. (2013). Anonymizing Health Data: Case Studies and Methods to Get You Started. Sebastopol, CA, USA: O'Reilly Media, Inc see especially Chapter 9. Geospatial Aggregation: Dissemination Areas and ZIP Codes

information to a high degree.[51] Geomasking has become common in health research, and there exist a number of different techniques.[52]

As noted above, we feel that these geomasking techniques are sufficiently refined to allow for good maps that can adequate inform people of radon levels at the neighbourhood level, and which can allay any residual privacy fears around public dissemination of radon data.

8. Publicly Held Databases—Protections and Release Issues

Organizations (that continue to be concerned about radon data having a privacy interest) may also worry about what happens once data passes into the hands of public databases. Organizations should take reassurance that they can ask for (indeed the law directs them to use) data sharing agreements, which will include language about release of any personal information to the public. However, we did hear concerns that the broader public, through Freedom of Information requests, might still get access to information with continuing privacy interest. This not an entirely implausible concern, in that all provinces, territories and the federal government have laws that allow members of the public to apply to government for release of information. While freedom of information legislation also includes protection of personal information from release, there are also exemptions from these protections—often in the name of the "public interest". However, and as we will now discuss in more detail, we do not think these provisions will result in radon data being released at the level of granularity of street address or GPS coordinate.

a. Confidential Information Harmful to Business Interests

The first reason to doubt radon information tied to address would be released is that there is a further ground—beyond privacy/personal information concerns- for it to be protected from release. All Canadian freedom of information legislation provides that a public body must not, generally release commercial, financial, labour relations, scientific or technical information that is supplied by a third party in confidence and which, if released, might harm business interests.[53]

---

[51] Armstrong, M.P., Rushton, G. and Zimmerman, D.L., 1999. Geographically masking health data to preserve confidentiality. Statistics in medicine, 18(5), pp.497-525. see also Stinchcomb, D. 2004. Procedures for Geomasking to Protect Patient Confidentiality. ESRI international Health GIS Conference October 19, 2004.

[52] Centers for Disease Control and Prevention, 2012. Cartographic Guidelines for Public Health. available at https://gis.cdc.gov/grasp/resources/CartographicGuidelinesPH2012508c.pdf accessed August 8, 2019. Zandbergen, P.A., 2014. Ensuring confidentiality of geocoded health data: assessing geographic masking strategies for individual-level data. Advances in medicine, 2014 Seidl, D.E., Paulus, G., Jankowski, P. and Regenfelder, M., 2015. Spatial obfuscation methods for privacy protection of household-level data. Applied Geography, 63, pp.253-263.

[53] Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 s.21; Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25 s. 16(1); The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s 19(1); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; s. 18(1); Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 17(1); Act respecting Access to documents held by public bodies and the Protection of personal information SQ A-2.1 s. 23; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6,s. 22(1); Access to Information

There is considerable interpretation of these provisions across Canada. Generalizing across jurisdictions it is difficult in that the statutory provisions are similar to each other, but tribunal decisions generally do not draw on interpretations from other provinces. The following is thus a compendium of commissioner/tribunal interpretations from diverse statutes.

- The legal provisions apply to information related to buying, selling or exchange of merchandise or services by profit-making as well as non-profit organizations, and applies equally to large and small enterprises.[54]This will not include information about prospective services and fees in a proposal but must be proprietary information.[55]

- Scientific environmental sampling would be included as 'scientific' or 'technical' information. [56] Ontario decisions suggest scientific data relates to hypothesis formation and testing, and technical information is the product of professionals trained in applied sciences and mechanical arts. [57]

- The information must be supplied "In confidence", which means the parties resisting disclosure must establish that the supplier of the information had a reasonable expectation of confidentiality, implicit or explicit, at the time the information was provided. This expectation must have an objective basis, considering whether the third party communicated to the institution that it be kept confidential or otherwise treated it as such, not otherwise disclosed or available from sources to which the public has access, and prepared for a purpose that would not entail disclosure.[58] Materials that have 'in confidence' written on the materials will satisfy this test. [59]

- If a third party seeks to stop a public body from disclosing such records, they need to show a risk of harm from disclosure of the record that goes beyond mere possibility or speculation, but only need to show harm is probable, not inevitable.[60] Saskatchewan uses the test of whether the likelihood of harm is "genuine and conceivable".[61] Federal law follows the principle of "a reasonable

---

and Protection of Privacy Act, 2015, SNL, c. A-1.2 s. 39(1); Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5 s.21(1); Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s.14(1);, Access to Information and Protection of Privacy Act, RSY 2002, c 1 s.24(1); Access to Information and Protection of Privacy Act, SNWT 1994, c 20 24 (1) ; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20, s. 24(1) Access to Information Act, RSC. 1985. C-A1 at s. 20(1).

[54] Ontario (Finance) (Re), 2020 CanLII 42300 (ON IPC) "Order PO-4047" para. 118

[55] Order F2018-32 (Re), 2018 CanLII 86134 (AB OIPC) para. 14

[56] British Columbia (Agriculture and Lands) (Re), 2010 BCIPC 9 "Order F10-06" at para. 35;
British Columbia (Environment Climate Change Strategy) (Re), 2019 BCIPC 13 "Order F19-11" at para. 17

[57] Ontario (Environment and Climate Change) (Re), 2015 CanLII 8309 (ON IPC) "PO-3459"at para .14
Ontario (Environment, Conservation and Parks) (Re), 2020 CanLII 28631 (ON IPC) "Order PO-4039" para. 11;

[58] Ontario (Finance) (Re), 2020 CanLII 42300 (ON IPC)"Order PO-4047" para. 122

[59] Order F2018-32 (Re), 2018 CanLII 86134 (AB OIPC) para. 18

[60] Ontario (Finance) (Re), 2020 CanLII 42300 (ON IPC) "Order PO-4047" para. 123. Merck Frosst Canada v. Canada (Health), 2012 SCC 3 (CanLII) at para. 94. See also Financial Institutions Commission (Re), 2013 BCIPC 2 (CanLII)("Order F13-02") at para 37.

[61] Saskatchewan (Environment) (Re), 2015 CanLII 29849 (SK IPC) para. 34

expectation of probable harm".[62] There must be a confident and objective evidentiary basis.[63] Evidence of such harm is likely to be uniquely within the knowledge of the Third Party, making it unlikely that there will by evidence to directly contradict that offered by the Third Party.[64]

- All applicable statutes provide an exception where consent is obtained from the third party.[65] As well, where a government body contemplates releasing such information, they have a duty to notify the third party.

- The exemption will not apply where a government agency has the power to compel a third party to produce records [66]

We were able to find prior decisions where privacy commissioners/tribunals excluded environmental sampling and research data supplied by third parties from disclosure.[67]

We do not think that there should be much issue that location-specific radon data, delivered by organizations pursuant to research sharing agreements, will be exempt as third-party records. The data sharing agreements can be explicit around expectations of confidence and specify any maps released be anonymized—and the anonymized data will likely serve the purposes of whomever requests data to be disclosed. If organizations do have to adjudicate the issue, they are unlikely to face a difficulty in showing the data is technical information. Radon data is produced by technical staff in laboratories. The data sharing agreements can be explicit around expectations of confidence. Organizations can argue that their relationships with their clients and reputation depends on homeowners trusting them not to publicize data specific to their homes, and any further data sharing with government would be jeopardized by an unwanted disclosure. Anonymized data will be severable from data linked to address, and a commissioner/tribunal should find that it would suffice for the public.

---

[62] Merck Frosst Canada Ltd. v. Canada (Health), [2012] 1 SCR 23, 2012 SCC 3 (CanLII) para. 192-199
[63] Vancouver Coastal Health Authority (Re), 2007 CanLII 35476 (BC IPC) ("Order F07-15") Abbotsford (City) (Re), 2013 BCIPC 27 ("Order F13-20")
[64] Canadian Pacific Railway v. British Columbia (Information and Privacy Commissioner), 2002 BCSC 603 at para 85
[65] Access to Information Act, RSC 1985, c A-1s. 20(5)Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165, s. 21(3); Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25 s. 16(3); The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s 19(2); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; s. 18(3)(a); Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 17(3); Act respecting Access to documents held by public bodies and the Protection of personal information SQ A-2.1 s. 23; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6,s. 22(3)(a); Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 s. 39(3)(a); Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5 s.21(4); Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s.14(3)(a); Access to Information and Protection of Privacy Act, RSY 2002, c 1 s.24(3); Access to Information and Protection of Privacy Act, SNWT 1994 s. 24(2)(a); Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20, s. 24(2)(a)
[66] Ontario (Environment and Climate Change) (Re), 2015 CanLII 8309 (ON IPC) "PO-3459"at para .26
[67] Ministry of Sustainable Resource Management, Re, 2003 CanLII 49176 (BC IPC)" Order 03-11"; Ontario (Environment) (Re), 2000 CanLII 20843 (ON IPC) "Order PO-1852"

b. Harm

Public sector freedom of information legislation typically provides an override of third party business or personal information: Governments may release information about risk of a significant harm, typically first notifying the person in issue.[68] In some provinces, the relevant statutes make this mandatory—such information must be disclosed.[69] Commissioners/tribunals have seldom found such circumstances to obtain, as evidence seldom shows the situation to be serious enough.[70] Applicants must generally provide some evidence that there is an actual risk of harm, and that the harm would be significant,[71] or a "an emergency-like circumstance"[72] with "a grave need with temporal urgency".[73] One decision held that disclosure might be triggered by information that discloses the existence, nature of, and extent of any harm that is anticipated if a risk comes to fruition, and information that allows the public to take action to avoid or mitigate the harm. The risk must be a prospective one, e.g. to enable people to take action.[74] These provisions are most appropriately used for episodes of individual, specific need for disclosure rather than generic arguments about social well-being. [75]

Tribunals have held such release is suitable for warning citizens about the release from prison of a violent offender [76] and to learn of family history of disease or disability that could affect the Applicant's health.[77] However, there are far more examples where the provisions have not applied. Some instances include: learning one's family history to help understand a diagnosed of hypoglycaemia and hepatitis C;[78] women in a city wanting to learning the reasons why a City Council resolved that the Mayor would not be permitted to meet or travel alone with any female employee of the City;[79] lists about high-risk employers in terms

---

[68] Access to Information Act, RSC 1985, c A-1 s. 20(6)(a), Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 s. 22(4)(b); Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25 s. 32(1)(a); The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s 29(2)(m); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; s. 17(4)(b) Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 42(1)(h); Act respecting Access to documents held by public bodies and the Protection of personal information CQLR, c. A-2.1 59(4),; Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6,s.33.1; Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 s. 9(3); Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5 s. 20(4)(b),31(1)(a) ; Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s. 30; Access to Information and Protection of Privacy Act, RSY 2002, c 1, s. 25(3)(b), s. 28; Access to Information and Protection of Privacy Act, SNWT 1994, c 20 s. 23(3)(b), 23(4)(b); 48(q); Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20 s. 23(3)(b), 23(4)(b); 48(q);

[69] Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25 s. 16(3); Act respecting Access to documents held by public bodies and the Protection of personal information CQLR, c. A-2.1 59(4); Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6,s.33.1; Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 s. 9(3); Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s. 30;

[70] College of Physicians and Surgeons of British Columbia (Re), 2019 BCIPC 2 at para. 20

[71] Energy Resources Conservation Board (Re), 2012 CanLII 70638 (AB OIPC) para. 21

[72] Southern Alberta Institute of Technology (Re), 2005 CanLII 78669 (AB OIPC) at para. 59; Alberta Health (Re), 2012 CanLII 70607 (AB OIPC) "Order F2012-14" para. 154

[73] College of Physicians and Surgeons of British Columbia (Re), 2012 BCIPC 14 para. 12-15

[74] Investigation Report F16-02, 2016 BCIPC 36 (CanLII), pp. 23

[75] School District No. 35 (Langley); School District No. 75 (Mission); School District No. 43 (Coquitlam); School District No. 38 (Richmond); School District No. 41 (Burnaby); School District No. 36 (Surrey); and School District No. 39 (Vancouver), Re, 1998 CanLII 2828 (BC IPC)

[76] Edmonton (Police Service) (Re), 2016 CanLII 82096 (AB OIPC)

[77] Nova Scotia (Community Services) (Re), 2010 CanLII 47110 (NS FOIPOP)

[78] Ministry of Children and Family Development, Re, 2001 CanLII 21591 (BC IPC) at para .25

[79] Fort St John (City) (Re), 2012 BCIPC 6 (CanLII)

of compliance with occupational health and safety standards[80] release of information that could assist in the investigation of a human rights complaint or stop discrimination[81] Information on aboriginal deaths in custody did not have the requisite temporal urgency.[82]

Radon exposure is typically chronic. Radon researchers we contacted as part of preparing this opinion could not identify a level which would count as requiring an urgent response. By extension there does not appear good scientific evidence to warrant governments treating a particular level as urgent. Very high test results in Pennsylvania have reached 37,000 Bq/m^3, 101,750 Bq/m^3 and 228,512 Bq/m^3.[83] In Canada, Health Canada found levels over 5,500 in two locations[84], and a recent large scale study in Alberta of 2382 homes found only one very high reading at 3441 Bq/m^3.[85] While these represent high *yearly* radiation doses (of between approximately 86 and 138 mSv per year[86]) it is unclear they require urgent or immediate action. Even with high radon levels, the appropriate response will typically be to notify the occupants of the homes, and this should be able to be done in a confidential manner. In most cases it should be sufficient to either warn the inhabitants directly or give notice to area residents without identifying precise locations. We thus do not contemplate situations in which government officials will be justified in giving precise locational radon information to persons other than immediate residents of affected properties.

c. Public Interest

Some provinces and territories' Freedom of Information legislation have what are called "public interest overrides".[87] In some cases, such as in Saskatchewan, Manitoba, and with the federal *Access to Information Act*, the override applies specifically against third party business interests and not directly against personal information.

---

80 Alberta Jobs, Skills, Training and Labour (Re), 2014 CanLII 23443 (AB OIPC) at para. 56
81 Athabasca University (Re), 2016 CanLII 85244 (AB OIPC)
82 Vancouver Police Department (Re), 2009 CanLII 63566 (BC IPC)
83 Tatu, C. 2016. Record High Level of Radon found in Lehigh County home. Morning Call. November 17, 2016. Available at https://www.mcall.com/news/breaking/mc-lehigh-county-high-radon-20161117-story.html accessed March 30, 2021
84 Loeiro, J., 2014. High radon levels found in Health Canada tests across country. CBC News, June 3, 2014. Available at https://www.cbc.ca/news/world/high-radon-levels-found-in-health-canada-tests-across-country-1.2662610
85 Stanley, F.K., Zarezadeh, S., Dumais, C.D., Dumais, K., MacQueen, R., Clement, F. and Goodarzi, A.A., 2017. Comprehensive survey of household radon gas levels and risk factors in southern Alberta. CMAJ open, 5(1), p.E255.
86 Based on calculations in Stanley ibid.
87Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 s.25(1)(b); Freedom of Information and Protection of Privacy Act, RSA, 2000 c. F-25 s. 32(1)(b); The Freedom of Information and Protection of Privacy Act SS 1990-91, c. F-22.01 s 19(3) (limited to third party records); The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175; s. 18(4)(restricted to disclosures harmful to business interests); Ontario's Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 23; A public interest override was not found for Quebec. Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6,s. 22(5) (restricted to disclosures harmful to a third party's business or financial interests); Access to Information and Protection of Privacy Act, 2015, SNL, c. A-1.2 s. 9(1),(2); Freedom of Information and Protection of Privacy Act , SNS, 1993, c. 5 s. 31(1)(b), ; Freedom of Information and Protection of Privacy Act, RSPEI 1988, c F-15.01, s. 30(1)(b); not found for Yukon, ; Access to Information and Protection of Privacy Act, SNWT 1994, c 20 48(s)(i) ; Access to Information and Protection of Privacy Act, SNWT (Nu) 1994, c 20; 48(s)(i) There is only a limited override for some information in the Access to Information Act, RSC. 1985. C-A1 at s. 20(6). For a critique see Information Commissioner of Canada, 2015. Maximizing Disclosure. Available at https://www.oic-ci.gc.ca/en/resources/reports-publications/2015-chapter-4-maximizing-disclosure

To be of public interest, the subject matter must be shown to be one inviting public attention, or about which the public has some substantial concern because it affects the welfare of citizens, or one to which considerable public notoriety or controversy has attached.[88] The category of public interest is thus broader than the override for urgent health and safety issues. Urgency is not required. [89] However, a potential disclosure must be, not just arguably in the public interest, but *clearly* (*i.e.*, unmistakably) in the public interest.[90] The term "compelling" is also used. [91]As such, the provisions should be interpreted narrowly.[92] British Columbia decisions say that the test is whether a disinterested and reasonable observer, knowing what the information is and knowing all of the circumstances, would conclude that disclosure is plainly and obviously in the public interest. As such, it is only intended to apply in serious situations, such as risk of harm to persons.[93] Ontario decisions appear to give greater leeway, and read public interest in terms of serving the purpose of informing the citizenry about the activities of their government, adding in some way to the information the public has to make effective use of the means of expressing public opinion or to make political choices. As such it can range to broader topics such as policy questions around the criminal justice system, operation of nuclear facilities, or contributions to municipal election campaigns.[94] Nova Scotia decisions are similar.[95]

Where the interest that might need to be protected is commercial, rather than personal privacy, the threshold is generally less stringent—business concerns not being treated as seriously as individual privacy concerns.[96] Ontario cases suggest the operative rule is whether the public interest in disclosure of the records clearly outweighs the purpose of the exemption.[97]

Privacy adjudicators also work to ensure no more information is released than is strictly necessary to serve the public interest. In Newfoundland and Labrador this is an express

---

[88] Grant v. Torstar Corp., 2009 SCC 61 (CanLII), [2009] 3 SCR 640 at para. 105.see also Nova Scotia (Office of the Premier) (Re), 2016 NSOIPC 15 "Investigation Report, IR16-01"at para. 45

[89] Office of the Premier and Executive council operations and Ministry of Skills Development and Labour, Re, 2002 CanLII 42472 (BC IPC)("Order 02-38") at para. 45; Alberta Jobs, Skills, Training and Labour (Re), 2014 CanLII 23443 (AB OIPC), "Decision F2014-D-01"at para 57

[90] Office of the Premier and Executive council operations and Ministry of Skills Development and Labour, Re, 2002 CanLII 42472 (BC IPC)("Order 02-38") at para. 45; Alberta Jobs, Skills, Training and Labour (Re), 2014 CanLII 23443 (AB OIPC)"Decision F2014-D-01", para 58-59; Alberta Health (Re), 2012 CanLII 70607 (AB OIPC)," Order F2012-14" at para. 192; Service Alberta (Re), 2018 CanLII 61327 (AB OIPC) "Order F2018-26" at para. 28 to 32; Prince Edward Island (Communities, Land, and Environment) (Re), 2016 CanLII 48836 (PE IPC)" Order No. FI-16-004" at para. 51 to 54

[91] Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 s. 23; Ontario Civilian Police Commission (Re), 2017 CanLII 45053 (ON IPC) at para. 45

[92] Calgary (City) (Re), 2001 CanLII 38149 (AB OIPC) at para. 72; see also Prince Edward Island (Communities, Land, and Environment) (Re), 2016 CanLII 48836 (PE IPC)" Order No. FI-16-004" at para. 51 to 54

[93] Investigation Report F16-02, 2016 BCIPC 36 (CanLII), pp. 26-27 see also Vancouver (City) (Re), 2017 BCIPC 45 (CanLII)("Order F17-41")

[94] University of Toronto (Re), 2007 CanLII 42222 (ON IPC) Order PO-2614; Ontario (Workplace Safety and Insurance Board) (Re), 2019 CanLII 14 (ON IPC)"Order PO-3915" at para. 43 to 47); Independent Electricity System Operator (Re), 2020 CanLII 36626 (ON IPC) "Reconsideration Order PO-4044-R" para. 85-90

[95] Nova Scotia (Office of the Premier) (Re), 2016 NSOIPC 15 "Investigation Report IR16-01 at para. 46-47

[96] Saskatchewan (Environment) (Re), 2015 CanLII 29849 (SK IPC); Saskatchewan (Environment) (Re), 2015 CanLII 46655 (SK IPC) Saskatchewan (Environment) (Re), 2014 CanLII 47921 (SK IPC)

[97] Independent Electricity System Operator (Re), 2020 CanLII 36626 (ON IPC) "Reconsideration Order PO-4044-R" para. 76; Cabinet Office (Re), 2020 CanLII 28080 (ON IPC)"order PO-4034" at para. 126

provision in the statute stating that a public body should disclose only the minimum amount of personal information necessary to accomplish the purpose for which is disclosed.[98] Ontario decisions show adjudicators will look to whether a significant amount of information has already been disclosed that can address any public interest considerations and refuse disclosing more. [99] In BC, the approach has been to say the public interest provisions relate to "information" rather than "records". The provision will be satisfied by an accurate summary of the information contained in the record.[100]

We think that a privacy commissioner/tribunal is likely to find that information about radon data is in the public interest. Indeed, radon creates clear risks to health that are avoidable with knowledge. Barring cases of extremely high radon readings (which we expect to be very rare), it is difficult to see that that the public interest extends to knowing radon readings at particular addresses. Anonymized data sets and maps will in almost all circumstances be sufficient.

9. Conclusion

We do not think that privacy law should be an obstacle to organizations sharing radon data. First and foremost, we do not think that radon data linked to address or GPS coordinate counts as personal information, and this should be enough to let the issue lie. To prepare for the off chance that the law evolves differently, we think that there are relatively easy steps that organizations can take to both share data and ensure compliance with privacy law. Organizations can prepare consent forms that anticipate future sharing of data with researchers. Any future sharing of data thus would come with consent (assuming participants agree). However, even in the absence of consent, data can still be shared for research purposes and subject to data sharing agreements. Such agreements can offer further layers of protection. Government agencies will be contractually obliged to agree to the terms. Moreover, the terms can stress that information is considered confidential and proprietary of the company, specifying that any radon data tied to address not be releases to the general public. Government agencies will also, as per freedom of information and privacy law, be further obliged to comply with the data sharing agreements. In the event that there is a request for radon data sets under freedom of information law, the organization will be notified and have an opportunity to participate in hearings. We also think that any broad public interest in radon data can be met through anonymized datasets and maps, which government agencies will be able to present as relevant information.

There is an outside chance that in cases of extremely high radon readings, provisions on notifying potentially affected persons may be triggered. In most cases organizations will already be notifying clients about test results. In some cases, it may be necessary to alert

---

[98] Access to Information and Protection of Privacy Act, 2015, S.N.L. 2015, c. A-1.2, s. 68.
[99] Ontario (Community Safety and Correctional Services) (Re), 2012 CanLII 18347 (ON IPC)("Order PO-3067) at para. 48 and 67); Independent Electricity System Operator (Re), 2020 CanLII 36626 (ON IPC) "Reconsideration Order PO-4044-R" para. 89;
[100] Investigation Report F16-02, 2016 BCIPC 36 (CanLII), pp. 26-27

neighbours (especially in condominiums or multi-family housing situations) and public health officials. There is a strong ethical basis for radon test companies to have such policies concerning radon data they hold—irrespective of whether the data is shared—as well as communicate the presence of such policies as part of data sharing agreements. In this way organizations can communicate results on their own terms and pre-empt any need for government agencies to do this.

Appendix A: FAQ for Industry

The following are questions frequently asked and responses based on this report that industry can use.

What is the purpose of sharing radon data?

Radon is a Class 1 carcinogen (known to cause cancer) according to the International Agency for Research on Cancer. Elevated radon concentrations expose humans to ionizing radiation and pose a danger to human health. Radon levels in homes and workplaces vary by region depending on multiple factors, including geology, soil conditions, and the design of buildings. Databases of indoor radon testing data can lead to better knowledge of radon and its health effects, including: Radon prevalence at the community level, the effects of radon exposure at the population level, the types of buildings susceptible to high radon, and the relationship of geological, soil conditions, and geography to radon exposure.

What data can be shared?

Radon researchers, database managers and mappers will likely want to know radon test results. This will help them to better understand the prevalence of high radon inside buildings and its geographical distribution. Many organizations also collect information about the type of tests, building types and age, and uses of the building (such as workplaces, schools or homes) which may be useful to researchers and others. The precise data to be shared should be discussed between organizations and researchers.

Under Canadian privacy law, there are limits on sharing personal information. For instance, an organization can collect data on people's names, where they live and their phone numbers as this is normally part of doing business. However, organizations cannot sell or gift this information to third parties. Our research suggests that information about building characteristics, include radon levels, is not personal information because it does not directly identify individual characteristics of persons. As such, information about building, including radon levels can be shared with third parties. If your organization would like further surety or wants to make sure people who have given you radon test results are not concerned, you can make sure radon data does not indicate specific addressed before sharing it. Our report describes ways to do that.

How is data shared?

Typically, researchers will want data sets as computer files which can be delivered electronically. These can be in the form of spread sheets, spatial data files or other reports.

The researchers will either work with the way your organization has already packaged the data or speak to you about other configurations.

Researchers will also enter into a data sharing agreement with you. This will specify the conditions under which data can be used and in what forms it may be shared with third parties or made public. Generally, data sharing agreements specify that no personal information will be made public.

How is personal information protected?

Radon information about properties is unlikely to be considered personal information. Four additional layers of protection are available to you.

First, data sharing agreements will specify that any personal information will be kept confidential and will not be shared with third parties or made public. Canadian public sector medical information researchers and databases are accustomed to high levels of privacy scrutiny and data security.

Second, you can also choose to adjust your data so that radon information cannot be traced back to individual addresses. Our report describes ways that data can be anonymized. You should discuss preliminary anonymization techniques with researchers to make sure you choose techniques that best facilitate their research objectives.

Third, researchers connected to governments are under strict requirements not to release commercial, financial, labour relations, scientific or technical information that is supplied by a third party in confidence and which, if released, might harm business interests. An organization can make clear to researchers that information is provided in confidence and that disclosure of radon test results linked to addressed to third parties or the general public would amount to a breach of confidence and potentially be harmful to business interests.

Fourth, any requests for release of information held by governments (such as through a Freedom of Information Request) must go through a legal process. Agencies generally must refuse to disclose personal information to an applicant if the disclosure is an unreasonable invasion of a third party's personal privacy. Generally, the data sharing agreement would be sufficient to establish that the information should not be disclosed. If a government agency still contemplates disclosing the information, you will be notified and have the opportunity to explain in writing why the information should not be disclosed. You will also have the right to appeal a decision of a government body to a Freedom of Information and Privacy Commissioner.

Are there any instances in which the data might become public?

There are provisions in Freedom of Information legislation for data to be released if strictly necessary to prevent harm to humans. Our scientific advisors could not imagine a situation where public disclosure of radon readings would need to be disclosed to the public. In all cases, high radon readings could be discussed directly with building occupants, or sufficiently delinked from location so as not to identify the original building. Even in an apartment building with extremely high radon readings, residents and public health officials could be notified through being told the general area.

We cannot entirely rule out the possibilities of a data breach. No system is entirely immune from human error or illegal activity. That said, we know of no instances where radon data has been leaked or where persons have sought to gain unpermitted access to radon data.

How do I respond to concerned homeowners who hear reports in the press of radon data being released?

There are many reasons why radon data might be released, including failure of radon organizations or researchers to put in place proper agreements and protocols. You can tell the press that your organization is committed to working within existing privacy laws, and that any sharing of data is strictly with researchers, database managers and mappers who work in the public interest to advance radon knowledge. All data is shared subject to data sharing agreements which are designed to protect personal information.

Appendix B: Sample Consent Form Wording for Radon Collection

By participating in this study/service, the participant agrees that this organization may collect and store information it receives on radon readings for specific locations, including the participants home or business location.

Any maps or publications made available by this organization to the public will use techniques to ensure your data is anonymous. This means that any documents or maps made available to the general public will not link radon data to any person or specific address. Members of the public will not be able to determine the radon levels of specific addresses or know which properties participated in radon measurements.

The participant agrees to allow this organization to share radon data with other organizations on the following terms:

1. Data will be shared on a confidential basis and in conformity with applicable law.
2. Data will only be shared with organizations which serve the public interest through advancing radon knowledge. This includes academic and other qualified researchers, government agency databases, and radon mapping entities.
3. Any sharing will be subject to data sharing agreements. These will specify that any data made available to the public will be anonymized. Any publicly accessible reports, databases or maps based on the information shared will not link radon data to specific people or addresses. Members of the public will not be able to determine the radon levels of specific addresses or know which properties participated in radon measurements.

Appendix C: Sample Data Sharing Agreement

The following is a copy of the BC Centre for Disease Control's (BCCDC) data sharing agreement for the British Columbia Radon Data Repository (BCRDR). The agreement was created in consultation with the BCCDC's privacy officer and Provincial Health Service Authority legal counsel. The agreement was signed with all contributors to the BCRDR, including the British Columbia Lung Foundation and Health Canada.

DATA SHARING AGREEMENT

British Columbia Radon Data Repository

This Data Sharing Agreement (the "Agreement") is dated for reference March 12, 2020,

BETWEEN:

The British Columbia Centre for Disease Control, a part of the Provincial Health Services Authority, a society established under the Societies Act (British Columbia) with offices at 655 West 12th Avenue, Vancouver, BC V5Z 4R4 Canada ("the Recipient")

AND:

[insert legal name of Provider, describe legal status of Provider] with offices at

[insert address of Provider]

("the "Provider")

(each a "Party", and collectively the "Parties")

BACKGROUND

A. The Recipient has a mandate in British Columbia to conduct public health surveillance, detection, treatment and prevention, including the provision of direct diagnostic and treatment services for people with diseases of public health importance; and

B. Environmental Health Services, a division of the Recipient, manages the British Columbia Radon Data Repository (the "Repository"), an integrated data set of indoor radon measurements from key stakeholders in British Columbia;

C. Radon is an environmental carcinogen that is influenced by geographic and built environment factors. Measurement of indoor radon in British Columbia has been done by a variety of organizations; however, public health surveillance has been limited by these datasets remaining mostly separate. To provide a more robust understanding of

indoor radon in British Columbia for public health planning, the Repository can merge currently disparate datasets and hold data collected into the future.

D. As such,the Provider has agreed to deliver to the Recipient a Radon Data Set,described in detail in Appendix A to this Agreement in order to support the Recipient's public health initiatives related to radon and its environmental risks.

THEREFORE in consideration of the mutual premises, covenants and agreements herein, the Parties agree as follows:

1. DEFINITIONS

1.1 For the purposes of this Agreement, including the appendices:

"Authorized Person" means a person approved by the Recipient to access the Data and/or the Combined Data;

"BCCDC" means the British Columbia Centre for Disease Control, a program of the Provincial Health Services Authority;

"CDR" means the Central Data Repository, a secure, limited access folder system controlled by the BCCDC, and which houses all datasets retained by the BCCDC which contain Personal Information and/or Personal Identity Information.

"Combined Data" means the combined data sets disclosed by all data providers to the Recipient which once combined will comprise of the data in the Repository;

"Data" means all elements of the Radon Data Set described in Appendix A to this Agreement, for inclusion in the Repository;

"Effective Date" means the date on which this Agreement has been signed by both Parties;

"FIPPA" means the Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c.165, as amended from time to time;

"Personal Identity Information" means "personal identity information" as defined in FIPPA;

"Personal Information" means "personal information" as defined in FIPPA;

1.2 In this Agreement, where applicable, a reference to the singular includes a reference to the plural and vice versa.

2. TERM

2.1 The Term of this Agreement shall commence on the Effective Date and will continue for five (5) years unless terminated earlier in accordance with this Agreement.

3. TRANSMISSION OF DATA TO THE RECIPIENT

3.1 The Data will be transmitted to the Recipient using a secure and approved method that meets the accepted policies and procedures of the Provider.

4. ACCESS, USE, DISCLOSURE AND RETENTION

4.1 The Recipient will ensure as follows:

i. that only Authorized Persons have access to the Data and to the Combined Data;
ii. that the Data and Combined Data are only used for the purposes set out at Appendix B to this Agreement unless the Provider has provided authority to do so;
iii. that no attempts are made to use the Data or the Combined Data to re -identify an individual; and
iv. that no linkage occurs other than as set out at Appendix B to this Agreement.

4.2 Except as expressly permitted in this Agreement, the Recipient will not,

i. sell, distribute or copy the Data or the Combined Data; or
ii. retransmit or combine the Data or the Combined Data with or into another database, without the written consent of the Provider.

4.3 The Recipient will retain the Data and the Combined Data in a secure, limited access folder system on its servers, accessible only by Authorized Persons based on the “need to know” principle.

4.4 The Recipient understands and agrees that no Personal Information that may be contained in the Data or the Combined Data may be accessed, stored, transmitted, or otherwise made available outside of Canada and that no person outside of Canada shall have access to the Data or the Combined Data in any manner except as expressly approved by the Provider in writing.

4.5 All requests for access and/or use of the Data or the Combined Data will b e processed in accordance with the procedure outlined in Appendix C to this Agreement.

5. CUSTODY AND CONTROL

5.1 The Data will be under the custody of the Recipient and under the control of the Provider.

5.2 The Combined Data will be under the custody of the Recipient, and data stewardship of the Combined Data will be done in accordance with the Recipient’s policies and procedures.

6. SECURITY AND PROTECTION OF PRIVACY

6.1 The Recipient will maintain the security and confidentiality of the Data and the Combined Data in its possession by making reasonable security arrangements and setting standards in

accordance with the Recipient's policies and procedures to mitigate the risks of unauthorized access, collection, use, modification of use, disclosure or dis posal.

6.2 The Recipient will maintain appropriate records regarding access approvals it grants to Authorized Persons.

6.3 The Recipient will identify to the Provider, upon request, the Authorized Persons responsible for managing the obligations of the Recipient under this Agreement, including the individual responsible for approving access for each Authorized Person and for maintaining appropriate records of all such approvals.

6.4 The Recipient will protect the confidentiality of all passwords, encryption keys and user accounts assigned by it in accordance with this Agreement, and in accordance with the Recipient's policies and procedures.

7. NON-DATA AND CONFIDENTIALITY

7.1 Notwithstanding the definition of "Data" and the agreed terms and conditions of this Agreement, if the Provider transfers written confidential information concerning the Data along with the Data, then to the extent permitted by law, the Recipient agrees to treat in confidence, for a period of ten (10) years from the date of its disclosure, any of the Provider's said confidential information. The Recipient's obligations of confidentiality do not extent to any information that:

i. can be demonstrated to have been publicly known at the time of disclosure; or
ii. can be demonstrated to have been in the possession of, or that can be demonstrated to have been, readily available to the Recipient from another source prior to the disclosure;
iii. becomes part of the public domain or publicly known by publication or otherwise, not due to any unauthorized act of the Recipient;
iv. can be demonstrated to have been independently developed, or acquired, by Recipient without reference to or reliance upon the Data submitted by the Provider under this Agreement; or
v. required to be disclosed by law, provided the Recipient takes responsible and lawful actions to avoid and/or minimize such disclosure.

8. PUBLICATIONS

8.1 If the Recipient intends to publish findings or distribute written materials based on the Combined Data, the Recipient agrees to only use aggregate or de-identified data in any such publication.

9. NOTICE OF UNAUTHORIZED ACCESS, USE, DISCLOSURE OR MODIFICATION OF DATA

9.1 The Recipient will notify the Provider immediately of any circumstances, incidents or events which to its knowledge have jeopardized or may in future jeopardize:

i. the privacy of individuals;

ii. the security of the Data or the Combined Data; or

iii. any suspected or apparent risk of a breach, or actual breach, of any term of this Agreement.

9.2 The Recipient will take all steps necessary to mitigate any of the circumstances outlined at 9.1 and the Provider reserves the right to proceed under a remedy for breach in accordance with [insert Provider policy if applicable, otherwise can remove this text].

10. REPRESENTATIONS AND INDEMNITY

10.1 The Provider makes no representations or warranties regarding the accuracy, completeness, reliability of fitness for use of the Data and submits that the Data is provided on an "as is" and "as available" basis.

10.2 To the extent permitted by the laws of British Columbia, the Recipient assumes all liability for damages the Recipient may suffer arising from:

i. the Recipient's acceptance, use, handling, storage or disposal of the Data;

ii. the Recipient's use of any results generated from the use of the Data,

except to the extent such damages are a direct result of the Provider's negligence or willful misconduct.

10.3 The obligations of the Parties under this section 10 survive the expiry or termination of this Agreement.

11. NOTICES

11.1 Any notice or other communication required or permitted to be given under this Agreement must be in writing and may be delivered by hand (including commercial courier), mailed by registered mail, or sent by fax or email to the address, fax number or email address of each party set out below:

11.2 Notice will be deemed to have been given on (i) the day the notice is hand delivered; (ii) three (3) business days after notice is mailed by registered mail; (iii) the day the notice is faxed or sent electronically provided the sender has received confirmation of transmission from the receiving party.

12. TERMINATION

12.1 Either Party may terminate this Agreement on no less than sixty (60) calendar days' written notice to the other Party.

12.2 Either Party may, by written notice to the other Party, immediately terminate the Agreement if the other Party a) breaches any term of the Agreement and the breach is not:

i. remedied within thirty (30) calendar days' of the receipt of notice from the first Party requiring it to remedy the breach; or

ii. capable of being remedied.

12.3 Upon termination of this Agreement for any reason, the Recipient will promptly remove the Data from the Combined Data, and return or destroy the Data, and then advise the Provider in writing to confirm the removal and return or the destruction of the Data.

12.4 The Recipient's obligations to maintain the privacy, security and confidentiality of the Data and the Combined Data will survive the termination of this Agreement.

13. GENERAL PROVISIONS

13.1 Nothing in this Agreement creates an agency relationship, a joint venture or a partnership between the Parties.

13.2 This Agreement will be binding upon and ensure to the benefit of the Parties and their respective successors and assigns.

13.3 If a term of this Agreement is invalid or unenforceable, said term will be severed and the remainder of the Agreement will remain in full force and effect.

13.3 Neither Party's failure nor neglect to enforce any rights under this Agreeme nt will be deemed to be a waiver of said Party's rights.

13.4 All terms which reference they survive the termination of this Agreement will survive the termination of this Agreement as well as any terms of this Agreement which, by their nature, are intended to survive the termination of the Agreement, will survive said termination.

13.5 This Agreement

i. is governed by the laws of the province of British Columbia and the laws of Canada applicable therein. Each of the Parties attorns to the exclusive jurisdiction of the courts of the province of British Columbia in respect of any matters arising out of this Agreement;

ii. including Appendices A, B and C, constitutes the entire agreement between the Parties as to the subject matter of the Agreement;

iii. may be signed in counterparts, and may be delivered by fax or email, all of which together evidence the same Agreement;

iv. may only be amended if agreed to in writing by both parties;

v. may not be assigned without the written consent of both parties.

IN WITNESS WHEREOF the Parties have executed this Agreement effective as of the Effective Date.

Provider	Per its authorized signatory: Name: Signature:
Recipient	Per its authorized signatory: Name: Signature:

Recipient Acknowledgement

Title: Date:

Title: Date:

I have read this Agreement. I understand the obligations of the Recipient and acknowledge my obligations as the lead of the BC Radon Data Repository as a Senior Scientist within Environmental Health Services.

Name: Sarah Henderson, PhD Signature: Date:

APPENDIX A
Data to be provided to the Recipient

[describe Provider data holdings covered under this agreement here]

APPENDIX B
Vision, Uses, Data Manipulation, and Data Linkage

A. Vision

The Repository is a provincial data repository housed on the Recipient's premises that includes all eligible radon samples collected by the Recipient to date, and will continue to include eligible radon samples collected from data providers in the future.

B. Accepted uses of data contained the Repository

Accepted uses of data in the Repository consist of:

i. public health surveillance of ecological radon exposure in British Columbia;
ii. Mapping of the distribution of indoor radon concentrations to support health protection and policy initiatives in British Columbia;
iii. Conducting research into a variety of radon-related purposes in British Columbia – for example, epidemiological, etc.

C. Procedure

Upon receipt of a radon data set from a data provider the following process applies:

i. the data set file is saved in the Recipient's central data repository – it is expected that data set files may be received in various formats including spread-sheets, spatial data files, reports, forms, etc. – any data set files received in the original format from a data provider will not be edited and will be considered to be the data provider's "Raw Original Files."

ii. the Raw Original Files will be examined by the Recipient to determine how the data is organized and what variables are present.

The table below shows the type of data sought by the Recipient and the variables that may be extracted from Raw Original Files – Note: the list below is not exhaustive – data providers may submit additional data elements.

Type of data	Example Variables
Core sampling information (required for inclusion)	● the radon concentration (in pCi/L or Bq/m^3) ● start date of measurement ● end date/duration of measurement ● six (6) character postal code ● in lieu of six (6) character postal code, an exact address or longitude and latitude coordinates
Methodology (desirable, but not required)	● testing device used (e.g., long-term alpha tracking monitors) ● testing device unique serial number ● reason for testing ● sampling strategy (e.g., convenience sampling) ● specific testing protocols
Building information (desirable, but not required)	● building use (e.g., residence, school) ● structural building type (e.g., low/ high rise) ● location of testing within building (e.g., basement, main floor) ● building square footage ● age of building ● number of windows ● heating system ● air conditioning ● separation between basement and main floor ● €building foundation

iii. Manipulate the Raw Original Files into a clean tabular format that will be considered a data provider's "Cleaned Data Files." All Cleaned Data Files will have an accompanying code to detail exactly what revisions and manipulations have been made. Cleaning steps relevant to all data received are listed in steps (a) to (d) below.

a. If any Personal Information or Personal Identity Information is found at this state, such information will be removed in this step in the procedure with the exception of the six (6) character postal code or the address or coordinates provided in lieu of it.

b. If an address is provided for an observation without a six (6) character postal code, pass the address string through the Government of British Columbia's

Physical Address Batch Geocoder to acquire the address' longitude and latitude coordinates. The address string would then be removed.

c. Acquire the longitude and latitude coordinates of each observation with a six (6) character postal code. The six (6) character postal code would then be removed.

d. To every observation's longitude and latitude coordinates, apply a random jitter to a degree inversely proportional to the location population density of the coordinates.

iv. Integrate the data provider's Cleaned Data Files into the Combined Data that holds Cleaned Data Files from all data providers. Only jittered longitude and latitude coordinates and geographic units of a reasonable minimum size (e.g., Community Health Service Area) would be included in the Combined Data as spatial variables. No variables that could be used to identify a data provider will be included in the Combined Data.

v. Assign a unique ID to each observation while keeping an internal record of how IDs were assigned. If a data provider decides to terminate this Agreement, this unique ID will support the removal of the data provider's observations from the Repository.

vi. As such, the Repository will retain:

i. the Raw Original Files from each data provider;
ii. the Cleaned Data Files that develop from the manipulation and revision of the Raw Original Files; and
iii. the Combined Data as outlined under this procedure.

D.Data Linkage

The Data, once submitted into the Combined Data, will be linked by general geographic area only.

APPENDIX C

Data Access Process and Release Procedure

A. Submitting a data access request

Access to the Combined Data in the Repository will be administer ed through the Recipient's data access request procedure - all requests can be submitted using the Data Access Request Template available on the Recipient's Data Access Request page at:

http://www.bccdc.ca/Health-Professionals-Site/Documents/Public%20Health%20Data%20Request%20Application%20Form%20201512 08%20-%20fillable.pdf

Requests for access to data contained in the Repository need to include, at minimum:

i. name of the Principal Investigator and team members on the project;
ii. a statement of the project objectives;

iii. a statement of the expected outcomes for the project.

B. Data Release and Re-identification Risks

The Repository contains six (6) character postal codes which is considered a quasi - identifier, that is a variable that creates re-identification risk. To mitigate this risk, prior to releasing information in response to a request, the Recipient will map all values according to the six (6) character postal code and add random jitter to the latitude and longitudinal coordinates, inversely proportional to the population density. This process aligns with the Recipient's Policy 110: GIS Mapping of Protected Health Information.

C. Request procedure

Once an approved request for data from the Repository has been received, the following procedure will be followed by the Recipient:

i. review the approved data request application and determine if any subsets to the Combined Data need to be made (e.g., requested only observations within a specified health authority region)

ii. extract data as per the request parameter, and make a record of this.

iii. review requested data against applicable Recipient data release policies (see part B above).

iv. send requested data accompanied by a metadata document to the requester via a Recipient approved method (i.e. Secure File Transfer)

v. create a folder for each request on the BCCDC CDR including the request, a file with a list of the Providers included in the request, and all material sent to fill the request along with any email communications related to the request.

D. Publication procedure

All publications and written materials to be distributed using the Combined Data must include the Recipient as a co-author.