Indigenous Mapping in the Cloud: A White Paper on Privacy, Ownership, Access and Security issues for First Nations using Google Geo-Tools

Rosanna Adams (UVic Faculty of Law) and Brian Thom (UVic Department of Anthropology)

Discussion Draft -- January 18, 2016

Table of Contents

First Nations use a range of technologies to assist in documenting their connections to and relationships with the land. Once this knowledge and cultural practices are documented, the data can be used in a range of applications from supporting indigenous governance decision-making to supporting cross-cultural understandings about indigenous territories, both within and outside of their communities. However, while geographic information and cloud-based technologies are beneficial because of their being affordable, accessible, and distributable -- there is a clear need to respect indigenous communities' concerns over privacy, security, ownership, control and access to their cultural heritage and knowledge.

From this position comes particular concerns over exploitation and misuse of cultural knowledge, and an articulation of the right to have First Nations own legal traditions respected. This paper will focus on how First Nations' may navigate these concerns when they connect their data with online tools like Google Earth or Google Maps. We will address the legal status of data and meta-data involved in utilizing Google's geo-tools and the implications of government access to this information. Though engaging with geo-tools brings risks of exploitation and misuse, the potential benefits provided by these services should not be discounted. Instead of suggesting that any risk is too dangerous for a First Nation to take or that a First Nation should blindly accept risks, this paper examines the legal framework surrounding online geo-tools in order to support conversations that can promote informed decision making.

Ownership, Access, Control and Possession

First Nations concerns about the exploitation and misuse of their traditional knowledge stems from the historical and current experience of misappropriation and exploitation,[1] which is connected to a lack of respect for Indigenous legal systems. When traditional knowledge is placed on the internet, respect for indigenous laws is needed not only by members of an indigenous community, but by everyone interacting with the traditional knowledge. An example of a First Nation in Canada asserting their own laws over intellectual and cultural property in the context of research is the National Aboriginal Health Organization's (NAHO) principles of Ownership, Control, Access, and Possession ("OCAP").[2] These principles are rooted in values of self-determination and inherent rights. The OCAP principles are intended to ensure that research involving First Nations does not cause harm to the First Nation, helps to increase research capacity and interest within the First Nation, and is beneficial and relevant to the community.

The OCAP principle of ownership is achieved when "a community or group owns information collectively in the same way that an individual owns their personal information".[3] Ownership can be contrasted with 'possession', ownership is about legal or 'principal stewardship', while "possession" is about literal or physical possession. In the context of data stored on a cloud server, in a local cloud, like Google's, the user may have possession and control, but in a large public cloud the user may have ownership but will not have possession. The NAHO asserts that when one party owns the data but another party possesses it, there is an inherent risk of abuse because ownership can not be easily asserted or protected.[4]

The principle of control is defined by the NAHO as control over "all aspects of research and information management processes which impact them".[5] Control is not about making a decision at one point in time, but it is the ability to control data at every point in time and to retain ultimate decision-making authority.[6] The principle of access is achieved by ensuring that all First Nations people "have access to information and data about themselves and their communities, regardless of where it is currently held".[7] The NAHO states that access must also involve being able to manage and make decisions about who has access to the collective information.[8]

OCAP has been used to develop legal frameworks that allow parties to clarify and codify in an enforceable form how information from research projects will be managed.[9] Research contracts are necessary because the default rules of Canadian intellectual property law and privacy law do not protect

---

[1] Department of Canadian Heritage, Respecting and Protecting Aboriginal Intangible Property: Copyright and Contracts in Research Relationships with Aboriginal Communities by Brian Thom (Ottawa: DCH, Copyright Policy Branch, 2006*)* at 10.

[2] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.

[3] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), at 4, online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.

[4] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.

[5] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), at 4-5, online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.

[6] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), at 5online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf> (This is expressed as having control over research "all stages of a particular project" including management practices, in terms of research. In the context of data being used on cloud computing this may translate into having control at each stage, for instance when the data is put online, when the data is accessed, how it is taken down.).

[7] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.

[8] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.

[9] See, cooperative language revitalization project between the Department of Linguistics at the University of Victoria and the Hul'gumi'num Treaty Group (HTG) [Department of Canadian Heritage, Respecting and Protecting Aboriginal Intangible Property: Copyright and Contracts in Research Relationships with Aboriginal Communities by Brian Thom (Ottawa: DCH, Copyright Policy Branch, 2006*)*]

First Nations' specific interests. Canadian laws codify and give enforceability to western legal and customary regimes. Canadian privacy legislation is focused on protecting "personal information", and is not tailored to protect community knowledge.[10] Canadian intellectual property laws are not about ensuring the appropriate transfer of information according to a First Nations' specific protocols and laws, but are about regulating the production of knowledge in a way that promotes the generation of wealth and encourages research.[11]

Canadian intellectual property laws protect a range of creations and inventions by assigning a bundle of legal rights to the creator or inventor. For example, copyright law protects the creator of an original work by giving the creator an exclusive right to produce or reproduce the work. Examples of copyrightable material include, "poem, painting, musical score, performer's performance, computer programs".[12] The inadequacy of intellectual property law to protect traditional knowledge can be seen to stem from the underlying commercial purpose of Canadian intellectual property laws.[13] For example patent and copyright protections have a time limit, which allows others to eventually utilize and benefit from the invention or work. This may be inconsistent with protocols that govern the transfer of traditional knowledge in First Nations communities. Further, intellectual property may work against First Nations by granting rights to those who collects, frames, or records traditional knowledge. Thus First Nations may need protection from intellectual property rights being asserted by outsiders.[14]

Intellectual property protection often requires a qualitative element, for instance copyright requires originality and patents require inventiveness. Thus though an original dance may be copyrightable, a dance that is linked in a certain way to a dance of an elder, may not be sufficiently original for protection under copyright.[15] The problem is thus two fold, the things contained in the category of traditional knowledge do not 'fit' perfectly within the category of things protected by intellectual property laws, and the protections granted by intellectual property law are not the same as the protections First Nations desire for their traditional knowledge.

Though Canadian law does not by default include First Nations legal orders, there is room for First Nations to design contracts that support their own proprietary laws and protocols. The contracts governing the use of Google services are pre-written without First Nations input. To demand that Google create individualized contracts to suit each users needs, may not be technically or economically feasible. Thus, instead of the management of data being governed by the idea of informed consent, as it would in a research situation, the burden is on First Nations to understand and accept a contract in a 'buyer-be-ware' framework. It is important to both strive to make First Nations legal orders more apparent in the realm of Internet services and to explore how First Nations may navigate and understand the current terms of contract.

---

[10] https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (The Canadian federal legislation PIPEDA controls how private-sector organizations use and share personal information, The *Privacy Act* governs the federal governments collection, use and disclosure of personal information.)

[11] Robert G Howell and Roch Ripley, "The Interconnection of Intellectual Property and Cultural Property (Traditional Knowledge)" in Catherine Bell & Robert K Paterson eds, *Protection of First Nations Cultural Heritage: Laws, Policy, and Reform* (Vancouver: UBC Press, 2009) 223 at 227.

[12] Canadian Intellectual Property Office, *A Guide to Copyright,* online: Canadian Intellectual Property Office <http://www.cipo.ic.gc.ca/eic/site/cipoInternet-Internetopic.nsf/eng/h_wr02281.html>.

[13] Robert G Howell and Roch Ripley, "The Interconnection of Intellectual Property and Cultural Property (Traditional Knowledge)" in Catherine Bell & Robert K Paterson eds, *Protection of First Nations Cultural Heritage: Laws, Policy, and Reform* (Vancouver: UBC Press, 2009) 223 at 225.

[14] CyberCart and TK, page 288.

[15] Robert G Howell and Roch Ripley, "The Interconnection of Intellectual Property and Cultural Property (Traditional Knowledge)" in Catherine Bell & Robert K Paterson eds, *Protection of First Nations Cultural Heritage: Laws, Policy, and Reform* (Vancouver: UBC Press, 2009) 223 at 226-228.

Google Geo-Tools

Google's Geo-tools are a wide range of programs that utilize mapping technology to display geographic information.[16] They allow users to develop products from Google's extensive base map. For instance, Google Fusion Tables turns a spreadsheet containing locations into a map, allowing a user to spatially visualize data points. Projects such as documenting land use and occupancy, sharing stories that are intrinsically connected with place, or revitalizing place names, are well suited to geo-tools as these programs excel at sharing knowledge that has a geographic element.

Many (but not all) of Google's geo-tools utilize a technology called "cloud computing" to create accessible and collaborative tools. Cloud computing refers to the remote storage of data made accessible through the Internet. Cloud computing is advantageous because it allows for a document to be accessed from many locations simultaneously. For instance, a user can upload a photo or edit a group document on their phone, and a second user given access to the document may then access, and even edit or download, the document from a different location. The accessibility of cloud computing can be invaluable to communities spread over large areas as projects may be developed communally without participants having to be on the same computer.

Cloud computing most often occurs through a public cloud where multiple users share data on a server owned by a service provider.[17] 80% of cloud services are provided by Amazon, Google, Microsoft, and Salesforce – which provide cheap, convenient, and reliable services. Srinivasan argues that because of these companies' large market share and focus on low-risk services, they have not needed to grow security practices.[18] Though security may be crucial to some users, there is a need to consider the extent to which absolute security is necessary for the overall objective of the user.[19] Google does not make absolute promises to its users about preventing unauthorized access, but the limited protection it offers may be sufficient in some circumstances.

First Nations have a long-standing concern about researchers coming to their communities, taking knowledge, and not returning anything to the community.[20] This fear is magnified in the context of cloud computing as users of Google's geo-tool open themselves up to the risk of anyone on the Internet being able to access the data they have stored on the cloud service and making unfair, unjust, or illegal use of the data. However, many of Google's geo-tools allow users to set the accessibility of a document to either public, protected, or private. Concerns also arise when considering that the servers that store cloud-based data can be hacked into (a problem with any platform), and that Google can be compelled by legal authority to surrender information. These issues can be problematic for First Nations when the data involves traditional knowledge. Traditional knowledge refers to a collection of intangible items or features and the integration of these features into the living cultural system of a community. Communities often have prescribed protocols for the use, protection, and preservation of their traditional knowledge.[21] While cloud-based tools offer platforms for information provision and advanced functions to share and collaborate, they are a potentially insecure place for storing sensitive data. The question that First Nations ask is not necessarily how they can fit TK into Canadian systems of ownership – but how they can maintain community control of the information and prevent exploitation.[22]

---

[16] The tools discussed in this paper are. Google Map Maker, which allows a user to edit Google's base map, Google Tour Builder, Google Earth, and Google Fusion Tables.

[17] http://www3.brandonu.ca/library/CJNS/22.2/cjnsv.22no.2_pg361-398.pdf, 364
S Srinivasan, *Cloud Computing Basics* (New York: Springer, 2014) at 83.

[18] S Srinivasan, *Cloud Computing Basics* (New York: Springer, 2014) at 85-86.

[19] S Srinivasan, *Cloud Computing Basics* (New York: Springer, 2014) at 84.

[20] **Forests for the Future: The View from Gitkxaala, pg 8**

[21] Robert G Howell and Roch Ripley, "The Interconnection of Intellectual Property and Cultural Property (Traditional Knowledge)" in Catherine Bell & Robert K Paterson eds, *Protection of First Nations Cultural Heritage: Laws, Policy, and Reform* (Vancouver: UBC Press, 2009) 223 at 225.

[22] CYberCart and TK, Chapter 19, page 290

A common problem flowing from the concern about inappropriate use of TK is what data to include in a mapping project and to what extend as the more precise the information included. For example, if specific locations of medicinal plants are mapped – there is a risk that persons without knowledge will harvest them improperly, running the plants for future users.[23] A potential remedy for this situation is to map sites as large polygons, but diminished detail may make a map less useful for First Nations who are interested in creating functional community tools.

A person who understands the context of a map would be able to see that even if only a salmon fishing spot was marked on the map, that the entire watershed is necessary for the continuation of the specific site. Someone who does not understand the context of the information may assume that the only important spaces are the ones indicated on the map. In the past the government has leaned towards site-specific recognition of Aboriginal right and title, and assume that blank spots are unimportant and do not require consultation with First Nations.[24] In 2014 the Supreme Court of Canada stated that the postage stamp approach was inappropriate for Aboriginal title claims,[25] but its recent use may give First Nations fear that making public maps that contain blank space will result in government excluding them from important decision making processes.

A recent example of the problems of sharing geographic data comes from the co-management of the caribou hunt in James Bay. Here the MLCP's opening of the caribou hunt in Cree traditional territory to sport hunters began with engagement and geographic information sharing from the Cree, Naskapi, and Inuit, but ended poorly with disrespect of the First Nation groups, caribou, and the land. The Cree cited many problems with sport hunters that had gained access to their lands including "careless disposal of remains, lack of enforcement, and interference with Cree customary practices".[26] Another problems was a lack of respect around Cree camps and cabins. The MLCP failed to indicate the location of camps and cabins through signage because they felt it may create a risk of vandalism and theft – but their approach lead to unsafe shooting by sport hunters around these areas, limiting Cree access to land during the sport hunt.[27] In the long term this policy has not stopped theft from Cree camps and cabins.[28]

Relationship to place is centrally important to many First Nations. Colonization often involves a destruction of the place relationship and participatory mapping can be a way to build back these relationships as well as ensure that TK is preserved.[29] Natural resource development critically affects First Nation's culture and relationship to land, being able to have control in this context is necessary to rebuilding First Nations "social fabric, culture, and traditions".[30] Mapping projects can allow a First Nation to communicate how they use their land, to show continuity with past practice, and to share knowledge of sustainable relationships to land with others utilizing shared resources.[31] Mapping projects

---

[23] http://www3.brandonu.ca/library/CJNS/22.2/cjnsv.22no.2_pg361-398.pdf, 377
[24] http://d3n8a8pro7vhmx.cloudfront.net/ubcic/legacy_url/950/Tobias_whole.pdf?1426350787, 23
[25] *Tsilqhot'in Nation v British Columbia*, 2014 SCC 44 at 60.
[26] Colin Scott & Jeremy Webber, "Conflicts between Cree Hunting and Sport Hunting: Co-Management Decision Making at James Bay" in Colin Scott eds, *Aboriginal Autonomy and Development in Northern Quebec*-Labrador (Vancouver: UBC Press, 2001) 149 at 161.
[27] Colin Scott & Jeremy Webber, "Conflicts between Cree Hunting and Sport Hunting: Co-Management Decision Making at James Bay" in Colin Scott eds, *Aboriginal Autonomy and Development in Northern Quebec*-Labrador (Vancouver: UBC Press, 2001) 149 at 161.
[28] Colin Scott & Jeremy Webber, "Conflicts between Cree Hunting and Sport Hunting: Co-Management Decision Making at James Bay" in Colin Scott eds, *Aboriginal Autonomy and Development in Northern Quebec*-Labrador (Vancouver: UBC Press, 2001) 149 at 165.
[29] Jon Corbett, "'I don't come from anywhere': Exploring the role of VGI and the Geoweb in rediscovering a sense of place in a dispersed Aboriginal community" in D Sui, M Goodchilld & S Elwood, eds, *Crowdsourcing Geographic Knowledge Volunteered Geographic Information (VGI) in Theory and Practice.* (Springer, 2012) 223 at 226-228.
[30] Jon Corbett, "'I don't come from anywhere': Exploring the role of VGI and the Geoweb in rediscovering a sense of place in a dispersed Aboriginal community" in D Sui, M Goodchilld & S Elwood, eds, *Crowdsourcing Geographic Knowledge Volunteered Geographic Information (VGI) in Theory and Practice.* (Springer, 2012) 223 at ##.
[31] Gitkxaala, 9-10

are an organizing tool for the "collective memory" of First Nations communities and may be a cognizable way to present information to non-land based individuals.[32] Maps can be used by First Nations as evidence to base demand participation in resource management decisions and as evidence in Aboriginal title claims.

Through *Haida Nation v British Columbia (Minister of Forests)*,[33] the Supreme Court of Canada outlined the Canadian government's duty to consult First Nations. The duty to consult arises when "the Crown has knowledge, real or constructive, of the potential existence of the Aboriginal right or title and contemplates conduct that might adversely affect it".[34] The scope of the duty to consult is "proportionate to a preliminary assessment of the strength of the case supporting the existence of the right or title, and to the seriousness of the potentially adverse effect upon the right or title claimed".[35] A First Nation may fear that the duty to consult could be limited on the basis of map data showing an absence of information at a certain location. This may lead an agency to conclude that the 'strength of claim' in that area was minimal. With no strength of claim, there is no duty to consult because no right would be infringed.

Through legal duties, including the duty to consult, the crown is barred from simply taking action without considering First Nation's rights. The fact remains that in the absence of clear evidence it is the Crown whose claim gets priority. This means that knowledge of where a First Nation has sufficiently documented use of land and where it does not, is crucially important. This concern highlights the importance of reading geographic data about land in connection not only to use by people, but to other land. This fact may be obvious those who made the map and thus something not included, but with interpretative help this data may not be apparent to all viewers.

It seems that the Crown could, with access to a First Nation's Google geo-tool information make decisions about the existence and strength of their duty to consult to the detriment of a First Nation. A government agency could look at a First Nations' information stored on geo-tools and conclude that there is consistently white space in the area in question and the First Nation does not appear equipped to make a claim. This could lead to First Nations being more frequently excluded from resource and land based decision-making. But a failure to consult where there is a duty to consult is required can be remedied in court[36] - and the threshold for "real or constructive knowledge" that triggers a duty to consult is low.[37]

Though it is less likely that private or protected Google geo-tool information will make its way into decision-maker's hands, it is likely that public or accessible information will. A First Nation should be cognizant of the potential ways geographic information publically available on geo-tools can be interpreted. A possible safeguard for a First Nation would be to ensure publically available geo-tools officially linked to the First Nation do not have white space. For instance instead of simply marking fishing spots on a map, also shading in the rest of the traditional territory and indicating use. In this case the Crown could not as easily draw the conclusion that they had no real or constructive knowledge of the potential existence of an Aboriginal right. The Crown may still conclude based on the lack of detailed or specific information displayed by the First Nation that the Duty to Consult is not triggered because the Crown conduct would not adversely affect an Aboriginal right or that this information lead to a weak strength of claim assessment.

Legal Orders

When information is put online through one of Google's geo-tool services, there are multiple legal orders involved. First there are the pre-existing rules of intellectual property law and privacy law. Existing alongside this are the laws of a First Nation community. Modifying and affirming the validity of Canadian laws are the contracts between the uploading user, Google, and other users of Google's services.

---

[32]

[33] *Haida Nation v British Columbia (Minister of Forests)* 2004 3 SCR 511

[34] *Haida Nation v British Columbia (Minister of Forests)* 2004 3 SCR 511, para 35

[35] *Haida Nation v British Columbia (Minister of Forests)* 2004 3 SCR 511, para 39

[36] *Taku River Tlingit First Nation v. British Columbia (Minster of Environment)* 2014 BCSC 12788, para 54, (Standard of review for existence of a Duty to Consult is correctness).

[37] *Taku River Tlingit First Nation v. British Columbia (Minster of Environment)* 2014 BCSC 12788, para 54

Canadian laws are enforceable through Canadian courts. The internationality of the Internet and Google, and the resulting issues of conflict of law and jurisdiction can make enforceability difficult.[38] A First Nation's laws are generally not enforceable in their own right through Canadian courts, but may be enforced within a First Nation through social sanctions.[39]

The Canadian legal rights a user has over content before it is uploaded to Google depends on whether or not the user has intellectual property rights, or they have mere possession of the content. The contracts that govern the use of content uploaded onto Google's geo-tools act to modify these pre-existing bundles of rights – often by transferring rights to Google. The transfer of rights is possible because many forms of intellectual property rights may be reassigned through contract.[40] For instance, the additional terms of services for Google Map Maker grants a very broad license to Google to do almost anything with the uploaded content, including the ability to give third parties permission to use the content.[41] In contrast, Google Tour Builder's additional terms of service give Google the ability to police for inappropriate content but no rights to reproduce the content.[42]

When a user engages with Google geo-tools, the user gives Google two categories of data. The first is meta-data, data about the user and how they use the service. This includes private information such as name, location, and IP address, and use information including which services are used, browsing patterns, and users connected with. The second type of data is content. This could include things like images added to Google Maps, or the data points and narrative text that create a tour in Google Tour Builder. Users of Google's services give up some of their rights to control their data and meta-data by agreeing to Google's Terms of Service,[43] Privacy Policy,[44] and various user agreements that form the prerequisite to using Google's services. These contracts allow Google to profit from the free services it provides. As a necessary part of making targeted advertising revenue Google needs returning users, thus their products create a balance between profitability and various desirable features, such as security or retention of rights.

Metadata

First Nations' may have concerns over the use of both their data and meta-data. Users 'use' of Google services produces the personal meta-data that becomes Google's most profitable product – advertising revenue.[45] In 2013 Google made 50.58 billion USD in advertising revenue.[46] Meta-data and data can also be used by the Canadian government agencies to build profiles of individuals, groups or events. Use of Google services creates another 'forum' for a person to be monitored in, and one that has been used by government agencies. A contemporary example of Canadian internet surveillance of First Nations groups is the Canadian Security Intelligence Service's ("CSIS") monitoring of Idle No More.[47]

---

[38] (The controversy surrounding and discussion within the recent BCCA judgment, *Equustek Solutions Inc. v. Google Inc., 2015 BCCA 265*, demonstrates the difficulty of enforcing court judgements on the internet, specifically the challenges of issuing injunctions.).

[39] Department of Canadian Heritage, Respecting and Protecting Aboriginal Intangible Property: Copyright and Contracts in Research Relationships with Aboriginal Communities by Brian Thom (Ottawa: DCH, Copyright Policy Branch, 2006*)* at 1.

[40] (With some exceptions, for instance the moral rights in copyright may not be reassigned.

[41] Google Inc, *Terms of Service for Google Map Maker*, online: Google <https://www.google.com/mapmaker/intl/en/mapfiles/s/terms_mapmaker.html>.

[42] Google Inc, *Google Tour Builder Content Policy,* online: Google <https://tourbuilder.withgoogle.com/about/content_policy>.

[43] Google Inc, *Google Terms of Service*, online: Google <http://www.google.com/intl/en/policies/terms/>.

[44] Google Inc, *Privacy Policy,* online: Google <http://www.google.com/intl/en/policies/privacy/>.

[45] Christian Fuchs, "Web 2.0, Prosumption, and Surveillance" (2011) 8:3 Surveillance & Society 288 at 289.

[46] Elliot Vredenburg, "Notes Toward a Meteorology of the Cloud" (2015) 13:2 Surveillance & Society 238 at 285.

[47] Justin Ling, "Canada's spy agency helped prepare all-of-government approach in case Idle No More protests 'escalated': secret files" *The National Post* (25 January 2015) online: National Post <http://news.nationalpost.com/news/canada/canadas-spy-agency-helped-prepare-all-of-government-approach-in-case-idle-no-more-protests-escalated-secret-files>.

First Nations may also be concerned about the protections of content data because content may contain traditional knowledge that should not be seen by unauthorized persons. A final concern is the use of content data, by government officials, or other persons, in court proceedings or negotiators.

Google's use of meta-data is governed mainly by the initial Terms of Service and the Privacy Policy. Google is able to share certain forms of aggregated user data with third parties and to "process personal information on behalf of and according to the instructions of a third party, such as our advertising partners".[48] These provisions allow Google to commodify user data and make a profit from targeted advertising.[49] Fuchs suggests that the ability to commodify data and the limited ability of users to opt out of Google's revenue generating activities indicates that Google's ultimate goal is corporate gain.[50] A concern voiced by some First Nations in the research context is that they do not want unauthorized economic benefit to be derived specifically from their traditional knowledge.[51] In Google's advertising revenue model, the economic benefit is not derived from traditional knowledge but from aggregated personal data. This data informs what type of adds Google displays for the user, which Google gains revenue from per 'hit'. Though advertising revenue may still be problematic for some First Nations, the fact that it is not derived from traditional knowledge or cultural property may go some way to alleviate concerns. [we will need a more specific example of potential revenue from geo-tools here].

Content Data

First Nations may utilize Google's Geo-Tools in numerous ways; I will present three categories of First Nations use. Whilst each First Nation has a particular legal system and differing interests in knowledge potentially shareable through Geo-Tools, these categories attempt to delineate different degrees of information sensitivity – and corresponding safe behavior.

Use 1: Traditional Use Study

A traditional use study is typically used to prepare an evidentiary record for proving Aboriginal title and rights. To prove Aboriginal Title in the Canadian courts, an Aboriginal group must show that they occupied the land prior to sovereignty, that there was continuity of occupation, and that occupation was exclusive.[52] To demonstrate these elements, a group must compile data about their use of land – Google's Geo-Tools, importantly Google Earth and Fusion Tables, are powerful tools for both organizing and presenting this data. First Nations may also engage in treaty negotiations with both the provincial and federal levels of the Canadian government. The bargaining position of a First Nation in these negotiations is effected by their potential ability to prove title and rights in Court. Thus the information of a Traditional Use Study is useful for a First Nation beyond the litigation context.

In both of these situations the stakes are high; proving title or negotiating a good treaty legally affirms Aboriginal people's control of their territory and may provide for self-governance. Both processes are expensive, lengthy, and involve dealing with the Crown. The crown is legally required to 'act Honorably in its dealings' with Aboriginal people, but during court proceedings takes an adversarial position, and in negotiations the crown represents a range of interests. A First Nation gathers sensitive and extensive information for these processes and must be able to control its use throughout and after the processes.

Google Earth provides a relatively high amount of data control because the user has the option to store Google Earth data on their own hard drive or local server. If data is stored on a private hard drive or local server, then it is only available through connection to that device. This could mean a single computer, or if resources allow, on other computers attached to the local server. Though this increases control over the data, it also limits the sharing capacities that exist when cloud sharing is utilized. Local

[48] Google Inc, *Privacy Policy,* online: Google <http://www.google.com/intl/en/policies/privacy/>.
[49] Christian Fuchs, "Web 2.0, Prosumption, and Surveillance" (2011) 8:3 Surveillance & Society 288 at 290.
[50] Christian Fuchs, "Web 2.0, Prosumption, and Surveillance" (2011) 8:3 Surveillance & Society 288 at 290.
[51] BT (HTG project) 2006, at 3.
[52] *Delgamuuk v British Columbia*, [1997] 3 SCR 1010 at 143.

storage means that unlike with many other Google tools, the First Nation would also retain possession of the data, which limits some avenues of misuse.[53]

Use 2: Educational Context

First Nations engage with Google Geo-Tools to create educational tools and archive information. Tools may include MyMaps, Youtube, Google Fusion Tables and Tourbuilder. These tools provide easy and affordable ways to collect and share data through a range of formats. These tools are interactive and can be used communally through the Google Cloud. Google geo-tools store data in Google's cloud, this means that Google, not the First Nation has ultimate possession. As NAHO articulates, loosing possession of data opens up the possibility of misuse,[54] but it is this lack of possession that allows for the "access" advantages of cloud computing.

The potential product of Geo-tools are a wide range of things from museum exhibits to class-room learning tools. The information contained is often important to the community and the community may have protocols for its dissemination and use. This data may have implications for Aboriginal title and rights claims, but it the data is not geared to be used in the legal context.

Compared to the Traditional Use Study, here the focus is less on confidentiality, and more about setting parameters for sharing information that follows the First Nation's protocols.[55] For example a student may film and upload a video of an elder telling a story, and plot the locations the story talks about on a Google Tour Builder map. If the student uses Google Tour Builder to create this story, then the student has the choice of setting it as open to all, open to people who possess the URL, or open to a select list of users.[56] These options allow the student to consider how problematic it would be if the data was not used respectfully, and appropriately calibrate the amount of people who have access to the file. Google, with the exception of legal requests, will not circumvent the User's sharing settings by distributing the information in a way the user has not consented to. The concern may go beyond the use Google makes of information, to potential abuse by third party viewers who either do not understand the importance of the information or respect First Nations protocols.

Use 3: Improving Google's base map

"Google Map Maker" allows an individual to edit Google's base map. This is potentially valuable to a First Nation because First Nation reserves are often not well documented on Google's basemap. A well-documented basemap is important for a wide variety of reasons including improving the navigability of a location for residents and visitors, increasing the visibility of businesses, and making clear the location of public spaces. Because of Google Map's prevalence across multiple platforms, not being on the map can make spaces practically invisible.

When uploading content to Google Map Maker, the user is contributing to an explicitly public service – the information is available to any one who has access to Google Maps and should not be sensitive information. The contract a user enters into with Google when uploading content to Google Map Maker works to facilitate the crowd sourcing of map data and protect Google's ability to generate revenue from its services.[57] The contract grants Google a license to use the information beyond making it available on Google Maps. A First Nation would loose the ability to prevent Google from utilizing the name or location of a place once it is uploaded to the service. Under this license, the user does not get to say which uses of the content are acceptable, so long as they fall within the broad language of the license. This is

---

[53] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.
[54] First Nations Center, "OCAP: Ownership, Control, Access, and Possession" (Ottawa: National Aboriginal Health Organization, 2007), online: NAHO <http://www.naho.ca/documents/fnc/english/OCAP.pdf>.
[55] Cybercart and Traditional Knowledge Chapter 19, at 288.
[56] Google Inc, *Google Tour Builder Content Policy,* online: Google <https://tourbuilder.withgoogle.com/about/content_policy>.
[57] Google Inc, *Google Tour Builder Content Policy,* online: Google <https://tourbuilder.withgoogle.com/about/content_policy>.

explicitly not in line with the NAHO's principle of control because Google's ability to make decisions without specific consent means that the First Nation does not have long term control over the information management process.

Users are explicitly told to not upload creative expressions through Google Map Maker. The intended content is community knowledge or facts,[58] things that in the Western legal tradition are not protected by intellectual property law.[59] Community knowledge is often exactly the type of knowledge that First Nations wish to protect, thus care should be taken when using Map Maker.

Policing the Internet and use of Publically/Semi-Publically Available Content

Though Google's contracts and Canadian laws may provide legal protections for content, the actual enforceability of these mechanisms is not guaranteed. Where a First Nation has intellectual property rights, they are only effective if the First Nation can afford to enforce them. If a First Nation finds that a copyrighted work that they have made publically or semi-publically available, for instance a recording of a traditional dance publically uploaded on Youtube, is being improperly reproduced – the discovery alone is not enough to stop the violation. Though an email to the violating party explaining the violation may fix the problem, in order to stop a violation a First Nation may have to engage in a legal process. These processes often require expertise, time, and financial resources. As Canadian intellectual property and privacy laws do not necessarily 'match' up with First Nations legal practices governing the use of their traditional knowledge, a sufficient legal remedy may not always be available when a First Nation sees a violation of their traditional knowledge.

Google does not actively police all the content that is uploaded to its servers or the eventual uses of the content it hosts. The Terms of Service provide that Google will respond to copyright violations, and in the case of repeat offenders terminate accounts.[60] This process requires that a complainant submit a documented legal request to Google.[61] Thus if a First Nation actively polices for the appropriate use of their content, it is possible that Google will help in this effort, but Google will only take down content that is illegal or violates its own terms of service. These policies are not necessarily in line with First Nations own legal systems for controlling the dissemination of TK.

[58] Google Inc, *Terms of Service for Google Map Maker*, online: Google <https://www.google.com/mapmaker/intl/en/mapfiles/s/terms_mapmaker.html> ("The Service is intended to reflect the local knowledge of users, and is not intended as a place for users to upload information obtained from third parties, such as directories, compilations, printed or online maps, or similar sources of information, including copyrighted content. Because the Service focuses on documenting factual information rather than creative expression, there are certain types of information that are not suitable for submission, and will not be accepted in the Service, as described below.").

[59] Robert G Howell and Roch Ripley, "The Interconnection of Intellectual Property and Cultural Property (Traditional Knowledge)" in Catherine Bell & Robert K Paterson eds, *Protection of First Nations Cultural Heritage: Laws, Policy, and Reform* (Vancouver: UBC Press, 2009) 223 at 228 (A patent can not be derived from something that is 'community knowledge' because it would already be in the public domain.).

[60] ("We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the U.S. Digital Millennium Copyright Act.").

[61] https://support.google.com/legal/topic/4556931?hl=en&ref_topic=3463371

Security against Government access to Private Content

A First Nation may be concerned about the Canadian Government's ability to access data on Google's servers that the First Nation has made "private" or "protected" through either a request to Google or hacking. As the Government is in a position to harm a First Nation through a misuse of land based data, the extent of protection from government access is important. Unfortunately there is virtually no quantitative data about how frequently and to what extent the Canadian government access private or protected content of First Nations stored on Google – due to legal requirements the statistics published by Google only indicate the number of requests in a time period but nothing about the content or target.[62]

Canadian government and public bodies' actions are governed by legislation and the *Constitution*. Content that is available publically on the Internet is not protected by section 8 of the *Charter*;[63] government agents are not breaching a reasonable expectation in privacy when they view Google geo-tool content that is public or to which they have the URL. But, due to section 8 of the *Charter,* Government agencies cannot usually hack into someone's Google account or ask Google for information relating to a user, without engaging in a legal process.[64] The risk that the Canadian government could access Google's data is real, but this risk should be qualified as legal and policy instruments limit the Canadian government's ability to access non-public information. Two possible avenues of access are Mutual Legal Assistance Treaties ("MLAT") and the Canadian Security Intelligence Service.

Mutual Legal Assistance Treaties

Google is an American company located in the US, thus Google is not automatically compelled to respond to Canadian government requests.[65] Canada does request information directly from Google, and is something successful. In order to have legal authority behind a request, Canada can make the request through the US government under the Canada-US Mutual Legal Assistance Treaty.[66] This allows a Canadian agency to request that the US Department of Justice "provide, in accordance with the provisions of this Treaty, mutual legal assistance in all matters relating to the investigation, prosecution and suppression of offences".[67] In order to request information Canada must be able to connect the information to a criminal offence. Further, an authority competent to make a legal request is a "law enforcement authority".[68] These provisions limit the scope of information that can be requested to information related to a criminal matter and the type of authorities that can request information.

The type of information produced is dependent on whether the order is equivalent to a subpoena, court order or search warrant. In order to access content, as opposed to meta-data, an agency would typically have to get a search warrant. This would require that the requesting authority provide information that meets a higher legal standard then required to obtain a subpoena or court order. If the Canadian law enforcement agency has the legal grounds to request a search warrant through the MLAT process, they may also have grounds to request a search warrant for a computer in Canada.[69] Thus though stored on a personal computer may seem safe – it is not necessarily safer from government access then

---

[62] https://www.google.com/transparencyreport/userdatarequests/CA/

[63] *Canadian Charter of Rights and Freedoms*, s 24(2), Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982 (UK)*, 1982, c 11.

[64] *R v Duarte*, see also C-51 backgrounder #2 at 13

[65] Google Inc, *Transparency Report, Legal Process*, online: Google <http://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond>.

[66] *Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters,* Canada and United States, 18 March 1985, Can TS 1990 No 19.

[67] *Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters,* Canada and United States, 18 March 1985, Can TS 1990 No 19 at Article II(1).

[68] *Treaty Between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters,* Canada and United States, 18 March 1985, Can TS 1990 No 19at Article VI(3)(a).

[69] R v Vu (note up case)

storage on a US provider's cloud. As the MLAT processes consume valuable time and resources,[70] orders are limited by criminal requirements, and Google does not automatically grant information requests, it is unlikely that the Canadian agency would pursue information from Google through an MLAT lightly.

The Canadian Security Intelligence Service

The Canadian Security Intelligence Service ("CSIS")[71] is the Canadian government agency responsible for collecting information on national security and disseminating the information to government agencies. Section 12 of the *Canadian Security Intelligence Act*[72] *("CSIS* Act*")* gives CSIS the mandate to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting *threats to the security of Canada* and, in relation thereto, shall *report to and advise* the Government of Canada".[73] "Threats to the security of Canada" is defined to exclude "lawful advocacy, protest, or dissent unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*)".[74] [emphasis added]

In 2014 the British Columbia Civil Liberties Association ("BCCLA") brought a legal complaint against CSIS for surveying three environmental groups. BCCLA argues that the actions the environmental groups engaged in were exercises of democratic rights, not security threats, and should not have been monitored.[75] The incident demonstrates that CSIS's interpretation of the provision mandating they do not spy on "lawful advocacy, protest, or dissent" is narrow. A wide range of surveillance may be legally justified by CSIS because of the 'conjunction' provision and the fact that CSIS also engages in 'preventative' surveillance. CSIS justifies spying on persons engaged in democratic activities because there is a chance that democratic activities may develop into domestic extremism. Early surveillance allows CSIS to "stay abreast of flashpoints or triggers".[76]

If the actions of a First Nation group or individual are suspected, on reasonable grounds, to fall within the definition of "threats to the security of Canada", CSIS is able to use its s 12 mandate to pursue an investigation against the person or group. The definition of threat does not just mean 'currently a threat', but also 'potentially a threat'.[77] This definition is broad enough to potentially bring non-threatening activities, like First Nations mapping projects under investigation if they can be considered to happen in conjunction with 'threatening activities'.[78]

CSIS's investigatory powers are initially limited by the *CSIS* Act and section 8 of the *Charter,* which protects against unreasonable search or seizure.[79] The CSIS Act requires that when the "Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada",[80] that the Director or employee then make an application for a warrant to the Federal Court. A warrant is generally required where a warrantless investigation would breach a reasonable expectation of privacy and violate section 8 of the *Charter*.

---

[70] Department of Justice, *Report of the Canada – United States Working Group on Telemarketing Fraud* (2000), <http://www.justice.gc.ca/eng/rp-pr/other-autre/tf/p3.html>.
[71] (Official website: https://www.csis.gc.ca/index-en.php).
[72] Canadian Security Intelligence Service Act, RSC 1985 c C-23.
[73] Canadian Security Intelligence Service Act, RSC 1985 c C-23 s 12(1).
[74] Canadian Security Intelligence Service Act, RSC 1985 c C-23 s 2.
[75] https://bccla.org/2015/08/i-was-spied-on/
[76] SHIRC 2012-13, at 25.
[77] Canada, Security Intelligence Review Committee, *Bridging the Gap* (Annual Report 2012-2013), (Ottawa: SIRC, 2013) at 25.
[78] Craig Forcese and Kent Roach, "Bill C-51 Backgrounder #2: The Canadian Security Intelligence Service's Proposed Power to "Reduce" Security Threats through Conduct that May Violate the Law and Charter" (12 February 2015), at 8, online: https://openmedia.ca/sites/openmedia.ca/files/C51_Backgrounder_Forcese_Roach_Part2.pdf.
[79] *Canadian Charter of Rights and Freedoms, s 8, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.*
[80] *Canadian Security Intelligence Service Act*, RSC 1985 c C-23 s 21(1).

When surveying Idle No More, a First Nations group, it appears that CSIS engaged mainly in monitoring through social networks and public forums.[81] This investigation would be similar to viewing an open Google Tour Builder Map or accessing a Google Fusion Table through a shared URL. It does not appear that a warrant was used in the Idle No More surveillance, or that it would be needed in the equivalent situation on Google's services. A warrant would likely be required for a CSIS s 12 investigation that uses intrusive investigative methods, including the interception of electronic communications or accessing private data.[82]

In order to obtain a warrant for this purpose, CSIS must satisfy the Federal Court that CSIS has followed the procedures as laid out in s 21. The warrant application must show that there are reasonable grounds to believe that the warrant is necessary for CSIS to investigate a threat to the security of Canada and that other investigative techniques are insufficient, impractical or unlikely to work.[83] If these two conditions are satisfied, then a Federal Court Judge may authorize a warrant.[84] In 2012-2013, 71 new warrants were received from the Federal Court of Canada and 165 warrants were replaced or renewed.[85] There is no specific data as to how many of these warrants were related to First Nations rights or governance issues.

With a section 21 warrant, CSIS may ask the Communications Security Establishment ("CSE") to engage in intrusive investigative methods. The legislation defining CSE's mandate only allows the CSE to direct its actions at Canadians or persons in Canada when the actions are taken under their "assistance mandate"[86] which allows for the provision of "technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties".[87] When CSIS has a section 21 warrant, they may task CSE to target a First Nation's data. The warrant can approve anything from hacking into a server to access data to asking a foreign intelligence agency for help in obtaining data – but must be approved by a judge. CSE's membership in the "Five Eyes" intelligence network means that even if CSE does not itself have the expertise to access Google's servers, it may be able to achieve this through another agency.

The Five Eyes Network – PRISM and MUSCULAR

The Five Eyes is a network of intelligence agencies from the United States, the United Kingdom, New Zealand, Canada, and Australia.[88] The most recent publically available version of the agreement governing the Five Eyes network is the 1957 UKUSA Agreement, which lays out a framework for maximum cooperation between the agencies and the exchange of products of various surveillance operations that relate to foreign communications.[89] In its 2010-2011 review of CSIS, the Security Intelligence Review Committee found that there was currently a "high level of cooperation between CSIS and its Five Eyes partner".[90] The Edward Snowden releases have provided evidence that members of the Five Eyes network have the capacity to access Google servers through a number of programs including MUSCULAR and PRISM.

---

[81] Justin Ling, "Snooping Idle No More", *Macleans* (2 September 2013) online: Macleans <http://www.macleans.ca/news/canada/the-spooks-werent-idle-either/>.
[82] 2014 CAF 249, 103.
[83] *Canadian Security Intelligence Service Act*, RSC 1985 c C-23 s 21(2)(b).
[84] *Canadian Security Intelligence Service Act*, RSC 1985 c C-23 s 21(3).
[85] Canada, Security Intelligence Review Committee, *Bridging the Gap* (Annual Report 2012-2013), (Ottawa: SIRC, 2013) at 18 (The number of warrants issued has increased annually, at least since 2008-2009).
[86] *National Defense Act*, RSC 1985 c N-5 s273.64(1)-(2) ("(2) Activities carried out under paragraphs (1)(*a*) and (*b*), (*a*) shall not be directed at Canadians or any person in Canada; and, (*b*) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.").
[87] *National Defense Act*, RSC 1985 c N-5 s 273.64(1)(c).
[88] James Cox "Canada and the Five Eyes Intelligence Community" (2012) Strategic Studies Working Group Papers at 4.
[89] UKUSA Agreement online: Nataional Archives, http://www.nationalarchives.gov.uk/ukusa/ at 4, 5
[90] Canada, Security Intelligence Review Committee, *Checks and Balances* (Annual Report 2010-2011), (Ottawa: SIRC, 2011) at 20.

PRISM is a intelligence program enabled by the *Foreign Intelligence Surveillance Act*[91] that allows the NSA to demand that an Internet service provider (ISP) give specified data to the NSA.[92] This data can include, "E-mail, chat, videos, photos, stored data, VoIP, file transfers, video conferencing, notifications of target activity – logins etc., online social networking details, and special requests.".[93] "Stored Data" could include both user meta-data and content stored on Google's cloud for the use of geo-tools. To begin targeting an individual the NSA must have a certificate authorized by the US Attorney General and Director of National Intelligence, and that has been reviewed for compliance with the basic requirements of the legislation by the Foreign Intelligence Surveillance Court ("FISC").[94] The legal requirements for a certificate can be said to be less rigorous then those required to obtain content information through an MLAT because there is no need requirement for an individual target.[95]

A certificate defines the category of persons that can be targeted under the certificate.[96] These people must be non US-persons and "reasonably believed to be outside the United States" and the purpose must be to "acquire foreign intelligence information".[97] A target does not have to be a suspected terrorist or a participant in any illegitimate activity, as a person may have foreign intelligence material regardless of their own activities.[98] An approved certificate allows the FBI to serve an ISP with a directive that indicates what the compelled ISP must give the government. [99] The communications provider would then have to provide the NSA with all the relevant data.[100]

MUSCULAR is run by the NSA, and Britain's SIGNIT agency, the GCHQ. The program involves the interception of data as it is transmitted between an electronic communications service provider's own servers. As a provider moves information internally between sever, GCHQ is able to redirect the data and hold it for three to five days. During this time period NSA then unpacks and decodes the data, then filters it through search functions.[101]

The NSA is able to conduct this program under the authority of Executive Order 12333 which authorizes the collection of all information for the purpose of "national defense" not prohibited by other applicable laws.[102] Because the point of 'interception' is outside of the United

---

[91] *Foreign Intelligence Surveillance Act,* 50 USC ch 36 § 1801 (1978)
[92] Barton Gellman and Ashkan Soltani "NSA Infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say" *The Washington Post* (20 October 2013) online: Washington post < https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story_2.html >.
[93] Ewen Macaskill and Gabriel Dance, "NSA Files Decoded" *The Guardian* (1 November 2013) online: The Guardian <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#doc/3>.
[94] 50 U.S. Code § 1881a(i)(2) (contains the 'reviewable' content of the certificate), 50 U.S. Code § 1881a(i)(3) (provides the type of orders the FISC may make).
[95] Donohue, 124
[96] Section 702 and Section 215 NSA Fact Sheet, at 1, online: Wyden, senate: http://www.wyden.senate.gov/download/?id=ea62ab96-06c3-4c0f-abc2-c2fd70776179&download=1.
[97] *Foreign Intelligence Surveillance Act,* 50 USC ch 36 §1881a(a)
[98] PCLOB report p 106, quoted in http://justsecurity.org/13124/pclob-report-questions-section-702/
[99] *Foreign Intelligence Surveillance Act,* 50 USC ch 36 §1881a(h)(1)(A), ("immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition;").
[100] PLCBO, 7.
[101] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say" *The Washington Post* (30 October 2013) online: Washington Post https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story_2.html.
[102] Ewan Macaskill and Gabriel Dance, "NSA Files: Decoded" *The Guardian* (1 November 2013) online: http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded. See Executive Order 12333 1.1(b), ("All means, consistent with applicable United States law and this Order, and with full consideration of the rights of united States persons, shall be used to develop intelligence information for the President and the National Security Council").

States and it is part of a lawful foreign intelligence investigation, no warrants or court orders are needed for the program per Executive Order 12333.[103] This program does not require the participation or even knowledge of an ISP to function.

The fact that intelligence operations can be run through foreign intelligence agencies, such as the five eyes network, is confirmed by a recent Federal Court judgement that clarified that CSIS does have the legal authority to seek assistance, through CSE, from foreign partners to intercept the communications of Canadians while they are outside of Canada, if there is judicial oversight.[104] The Federal Court has jurisdiction to issue these warrants "when the interception is lawful where it occurs".[105] What this judgement does not specifically state is that the Federal Court can issue a warrant that allows CSE to gain assistance when spying on a Canadian who is currently *within* Canada. This may be seen as against the 'rule' that international agreements will not be used to skirt domestic law, and the statement that the Five Eyes Network partners do not use the network to evade national laws.[106] But if it is the case that the Federal Court would grant a warrant for CSIS to pursue an investigation, and that they are merely seeking technical assistance to do what they otherwise would be legally allowed to do, then they would not be using a foreign agency to avoid domestic law. CSIS is not prevented from surveying Canadians, but is required to follow legal processes when it does.

Snowden Backlash

In the wake of the Snowden disclosures, changes have been made to the way US intelligence agencies conduct surveillance of US persons and dragnet surveillance. Changes in the US have lead to greater protection of US persons, but these changes do not aim to stop the US from being able to run programs that target Canadians. A similar move against overbroad surveillance can be seen in Canada, where civil liberties groups have opposed CSIS spying on Canadian's exercising democratic rights. But recent changes to Canadian legislation have decreased Canadians protections from surveillance. Bill C-51 has increased the powers of CSIS by giving it 'kinetic' powers to take measures to reduce security threats[107] and also increased the ability of specific government agencies to share information.[108] The combined effect of these laws is to increase the ways in which Canadians can be surveyed and the ways in which this information can be used. Surveillance in Canada has had an 'anti-terrorism' focus, but recently there has been publicity about the monitoring of First Nations and Environmental 'radicals'.

Google and other Internet service providers have been working for more transparency about intelligence gathering processes. When Google receives a request for information it will notify the affected user of the request if it is legally able to, but requests made pursuant to many FISA powers come with a gag orders preventing Google from notifying a user that the request has occurred.[109] In the wake of the Snowden leaks, Google and other internet service providers successfully challenged the gag order provisions. They are now able to publish the number of FISA orders in bands of 1000 with a 6-month delay. This brings their reporting abilities in regards to foreign intelligence more in line with their ability

---

[103] John Napier Tye, "Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans" (18 July 2014), online: Washington Post https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html., see also Executive Order 12333, s 2.5 (Here the order delegates power to the Attorney general to approve the any techniques that would require a warrant if undertaken in the US when a US person is involved or within the US – there is no mention for the requirement of an approval or warrant if the target is not within the US or a US person.)

[104] X (Re), 2014 CAF 249 para 87-89

[105] X (Re), 2014 CAF 249 para 103.

[106] James Cox "Canada and the Five Eyes Intelligence Community" (2012) Strategic Studies Working Group Papers at 23.

[107] C-51 backgrounder 2, 15, see also CSIS Act S 12.1

[108] *Security of Canada Information Sharing Act*

[109], http://www.google.com/transparencyreport/userdatarequests/faq/#cover_all_categories (Subject to reporting requirements, for instance if the request comes through a NSL or FISA order, Google can not disclose that the request has happened.)

to report in the context of criminal investigations.[110] Though this information is an important step towards transparency, it does not provide clarity as to what type of content is requested or the purpose it is used for. Thus there is no way of knowing how many of the requests from the Canadian government recorded on Google's website pertain to First Nations.

Google has stated that it does review information requests to ensure that the request "satisfies legal requirements and Google's policies",[111] and will seek to have requests narrowed if the request appears to be too broad.[112] This is supported by Google's published statistics on information requests granted. For instance in July to December 2014, of 100 Canadian information requests, Google produced some data for only 45% of the requests.[113]

Government Use of Content and Metadata

The fact that the Canadian government has the legal and technical tools to access Google geo-tool content in certain circumstances may be sufficiently problematic that a First Nation decides some content, should not be on the Internet in any form. An individual uploading content to a geo-tool may not be able to predict all the potential uses of that information; a seemingly innocuous piece of traditional knowledge may be used in an unforeseen way in a resource management decision. Corbett describes how the Tlowitsis First Nation's Treaty Advisory Team felt that if they lost control over land-based information on the internet it might "be transformed, used selectively, and reused in ways that at this point in time cannot even be imagined".[114] Though risks can be discussed, they can not all be imagined. Corbett argues that this fear is especially strong amongst First Nations communities in Canada because of the colonial history of appropriation and misuse of geographic data.[115]

The content of Google geo-tools is potentially dangerous because they contain spatial data about how a First Nation uses and relates to its territory. As Aboriginal title and rights are intrinsically connected to land and the use of land, spatial data is indispensable to land claims and natural resources management decisions as this information defines where an Aboriginal claim can be made and the type of claim that can be made. As the onus is on a First Nation to prove that they have specific relations to certain territories in order to access their rights, an absence of data or 'white space' on a map is potentially useful to a government agency. Control over who holds geographic data and how it is presented or understood is intrinsically linked to both the government and First Nations' bargaining positions for land based management decisions.

A First Nation must think carefully about what is public or accessible on the internet as government agencies are able to access this data, by setting data as private or protected a First Nation is not guaranteed absolute protection from government access, but strongly limiting the situations in which it might occur. Once Canadian agencies have data – its use is restricted by certain mechanisms. Canadian government agencies internal and external sharing of information is subject to restrictions, meaning that certain government branches may not have access to the same information as others. Finally, the situation

---

[110] Spencer Ackerman, "Tech giants reach White House deal on NSA surveillance of customer data" *The Guardian* (27 January 2014) online: The Guardian <http://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data>.

[111] http://www.google.com/transparencyreport/userdatarequests/legalprocess/#what_does_google_do

[112] "What does Google do when it receives a legal request for data? "http://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond"

[113] http://www.google.com/transparencyreport/userdatarequests/CA/, (Percentage of requests where some data produced for Canada range from 23% to 78%. This includes both legal requests and emergency requests)

[114] Jon Corbett, "'I don't come from anywhere': Exploring the role of VGI and the Geoweb in rediscovering a sense of place in a dispersed Aboriginal community" in D Sui, M Goodchilld & S Elwood, eds, *Crowdsourcing Geographic Knowledge Volunteered Geographic Information (VGI) in Theory and Practice.* (Springer, 2012) 223 at 234.

[115] Jon Corbett, "'I don't come from anywhere': Exploring the role of VGI and the Geoweb in rediscovering a sense of place in a dispersed Aboriginal community" in D Sui, M Goodchilld & S Elwood, eds, *Crowdsourcing Geographic Knowledge Volunteered Geographic Information (VGI) in Theory and Practice.* (Springer, 2012) 223 at 234.

in which the information was initially gathered may place restrictions on how the government can use data. These limitations on government use of data provide a framework for a First Nation to make informed decisions about the use of Google Geo-tools.

Mandate of Agency Restrictions

The potential capacity of the Canadian government agencies to access Canadian's internet data is limited by the legislated rules and policies governing these agencies. Generally the government cannot engage in random intrusive searches – for instance MLAT use is limited by the requirement of relation to a criminal investigation[116] and the statutory requirements for the CSIS section 21 warrant ensure proper justification for intrusive searches.[117] These requirements have the effect of preventing random searches of a First Nations internet data. The assurance provided by the Federal Court oversight of section 21 warrants may be limited by past instances when CSIS has lacked candor in this process.[118] Both of these restrictions only apply when the information sought is information that the user has an expectation of privacy for, thus government does not have restrictions in regard to accessible conduct – like a public Google TourBuilder document.

The NSA is subject to different, and significantly less strict controls when surveying Canadians then when surveying American citizens. American surveillance programs targeting and minimization procedures are put in place to protect US persons – not Canadians.[119] First Nations may be concerned about US government use of their data, but also about the potential that the NSA may transfer or make available data that would other wise be inaccessible to Canadian agencies or industry. The potential for data to be disseminated in this way is problematic because it would erode the protections granted by the 'criminal' and 'threat' requirements of the CSIS or MLAT process.

Information Sharing Amongst Government Agencies

Canadian government agencies have restrictions placed on their ability to share and access information. Depending on the expectation of privacy connected to the type information, only certain agencies may access the information and there may be restrictions on sharing the information. Canadian privacy laws, such PIPEDA and equivalent provincial legislation, regulate Government use of private personal information. This legislation may work to protect meta-data and information relevant to identifying a user, but it is not specifically designed to protect content data as this is usually non-personal.

Government sharing of non-personal information may also be prevented by an agencies governing legislation. The *CSIS* act imposes a general ban on CSIS from disclosing information gained through investigations. This is subject to several exemptions; CSIS may disclose information in relation to its mandated duties and in a list of enumerated situations.[120] The section 12 duty allows CSIS to "investigate…respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada".[121] Though a section 12 investigation may allow CSIS to access and retain Google geo-map content that was incidental to an investigation of a threat, the section 12 duty only allows CSIS to report to and advise the Canadian Government about threats to security. But one of the enumerated exceptions gives the Minister the power to disclose information to anyone in the federal public administration if the disclosure is of sufficient "public interest" to outweigh the invasion of privacy the disclosure could cause.[122] This is the

[116] FN7 WCGD
[117] R v Lising
[118] Colin Freeze, "CSIS not being forthcoming with court federal judge says", *The Globe and Mail* (25 November 2013) online: The Globe and Mail <http://theglobeandmail.com>.
[119] John Napier Tye, "Meet Executive Order 12333: The Regan rule that lets the NSA spy on Americans" (18 July 2014), online: Washington Post https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.
[120] Canadian Security Intelligence Service Act, RSC 1985 c C-23 s 19.
[121] Canadian Security Intelligence Service Act, RSC 1985 c C-23 s 12(1).
[122] Canadian Security Intelligence Service Act, RSC 1985 c C-23 s 19(2)(d).

only exemption whose use must be reported to a review committee, indicating that it is a 'special case' exemption.[123] Sharing information relevant to a First Nations land claim may be in the public interest, but if this information has been acquired through intrusive measures then it also involved a violation of privacy. The process that approved the section 21 warrant would have occurred on the basis that the purpose of the investigation was the investigation of a security threat. Just because a court approved the violation in the original circumstances of the investigation does not mean the violation would be justified for other purposes.

Though CSIS is subject to restrictions regarding who it can share information with, the recent Bill C-51 has acted to increase information sharing between government agencies by introducing the *Security of Canada Information Sharing Act*. This act allows any Government of Canada institution to share information on its own accord, or by request, with a Government of Canada institution contained in Schedule 3 of the act, subject to any legislative provisions.[124] Though the attorney general, the agency representing the government in land claim negotiations or title cases, is not on this Schedule, the legislation shows a trend towards unrestricted information sharing amongst Canadian government agencies.

While law enforcement and intelligence agencies are subject to strict regimes controlling the spread of information, other Canadian agencies are subject to different rules. Aboriginal Affairs and Northern Development Canada's "Aboriginal Consultation and Accommodation" guidelines explicitly encourage federal departments and agencies to share information about potential and established Aboriginal rights of Aboriginal groups across Canada.[125] Both Federal and Provincial Canadian governments keep databases of information on Aboriginal and Treaty rights relating to specific First Nations, that are readily accessible to government agencies and departments – but not accessible by the public.[126] Information publically available or accessible on the Internet through a shared URL may be placed into these databases through the work of government researchers. Once on a database the information is available to all departments having to make strength of claim or take duty to consult actions. A First Nation should be particularly careful about information that is publically available on the Internet and linked to the First Nation as it may end up in these databases.

Use of information in land based decision-making.

Depending on how a government intends to use information it must be collected and handled in a specific manner. Evidence in court is subject to exclusionary rules and must be relevant to a material issue in litigation. Today evidence derived from CSIS investigations is used in court more frequently than in the past. This shift has occurred partially because of the increasing overlap between criminal charges and CSIS investigations.[127] The inclusion of CSIS intelligence information in court rooms has mainly occurred in the realm of immigration or terrorism charges, not in aboriginal title claims.

Intelligence information's status as admissible evidence may be revoked if it is found to have been gathered in violation of the *Canadian Charter of Rights and Freedoms*. This is possible if CSIS pursues an intrusive investigation without a warrant or it becomes apparent that CSIS used the cloak of a threat investigation to pursue information for another primary purpose. In these circumstances a court may find that the evidence was acquired in a manner that violated the *Charter* right against unreasonable search and seizure.[128] If a *Charter* violation is shown, the evidence may be ruled inadmissible by *Charter*

---

[123] Canadian Security Intelligence Service Act, RSC 1985 c C-23 s 19(3).
[124] *Security of Canada Information Sharing Act* 5(1)
[125] http://www.aadnc-aandc.gc.ca/DAM/DAM-INTER-HQ/STAGING/texte-text/intgui_1100100014665_eng.pdf, 37
[126] http://sidait-atris.aadnc-aandc.gc.ca/atris_online/Content/Search.aspx (ATRIS is the Federal government system used to track Aboriginal treaty and right information)
[127] Kent Roach, "When Secret Intelligence Becomes Evidence" (2009) 47 Supreme Court Law Review 147 at 162, 186.
[128] *Canadian Charter of Rights and Freedoms*, s 8, Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982 (UK*, 1982, c 11.

s 24(2) which states that evidence that was obtained in violation of the *Charter* shall be excluded if it its inclusion would "bring the administration of justice into disrepute".[129]

Aboriginal land claims and natural resource decisions are often made outside of a court through negotiation or government decision making. In engaging with these processes a government agency is not generally bound by the court rules of evidence use, though there may be statutory requirements, common law requirements, or departmental policy. Inter-governmental sharing of information relevant to Aboriginal consultation is encouraged.

[129] *Canadian Charter of Rights and Freedoms*, s 24(2), Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982 (UK*, 1982, c 11.