Data Brokers

A Look at the Canadian and American Landscape

Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada

September 2014

Table of Contents

Abstract

The purpose of the research report is to provide an overview of data brokers and their operations based on the Canadian and American privacy environments.

Introduction

The practice of compiling and selling individuals' personal information by data brokers for marketing or other purposes raises privacy concerns. These concerns result, in part, from a lack of transparency and openness and the challenges individuals face in trying to exert control over their information.

These concerns and privacy risks go beyond the top-of-mind issues related to the impact of a data breach from databases that hold vast amounts of information. As noted by Daniel Solove: "*…the problem with databases and the practices currently associated with them is that they disempower people. They make people vulnerable by stripping them of control over their personal information.*"[1]

This paper is aimed at providing individuals and businesses with an examination of the privacy regulatory environment in Canada and the United States, and the privacy compliance requirements for data brokers based in other jurisdictions when doing business in Canada. As individuals are made aware of the privacy compliance requirements for data brokers operating in Canada, they will be better informed to exercise their consent and control choices. In addition, as data brokers have a better understanding of their privacy obligations, it should help inform their practices to support consumer control, trust, and transparency.

The paper is based, in part, on research on data brokers funded through the Office of the Privacy Commissioner of Canada's Contributions Program.

A. What Is A Data Broker? Setting The Scope

To categorically define a "data broker" has been difficult, as was recently demonstrated in a December 2012 United States privacy summit involving the Federal Trade Commission (FTC), lawmakers, and industry.[2] Are data brokers those organizations that trade in personal information without dealing with consumers directly? What of those companies that have direct relationships with individuals and use that information to create databases for marketing or other purposes?[3]

In recognizing the range of organizations and business models involved in the trade of information, the scope of this paper will be limited to the FTC definition: *"Data brokers are companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies."*[4]

B. The American Context

Legislation and Oversight - Environmental Scan

In the last few years there has been a growing interest in data brokers' practices in the United States.[5] This has been attributed to a lack of transparency concerning the practices of such organizations, low consumer awareness of the scope and existence of these practices, and the explosion of the ability of entities large and small to collect, store, and analyze data both offline and on, to create extremely detailed profiles.

There is no national, comprehensive private sector privacy legislation in the United States. Instead, multiple, and often overlapping state and federal statutes, regulations, and common law torts create a complex patchwork of privacy and data security requirements, but there is no comprehensive legislation that covers *all possible types of personal data* or *all of the business activities* of all data brokers. For example, nearly all U.S. states have a breach notification law, and there are federal breach notification requirements for certain personal health and financial data. Most states also have laws mandating reasonable information security, and as well as multiple state laws governing the use of specific data, such as health information, Social Security numbers, financial information, or biometrics, or providing certain privacy notice rights in an online context. At the federal level, privacy rights are similarly dispersed largely through sector-specific legislation, such as the *Fair Credit Reporting Act* (FCRA), the *Gramm Leach-Bliley Act* (GLBA), the *Health Insurance Portability and Accountability Act* (HIPAA), and the *Health Information Technology for Economic and Clinical Health Act* (HITECH), all of which contain some provisions related to privacy and data protection.

Generally, though, the U.S. statutes only protect consumers in limited circumstances. For example, the FCRA – which is the existing U.S. federal law that currently regulates a significant portion of the Big Data industry – applies only to that information which businesses receive from consumer credit reports, such as those related to credit, insurance, housing, and employment, and does not necessarily cover all data brokers' marketing activities.[6] In addition, the GLBA is limited to financial institutions in certain traditional banking and lending activities.

The broadest U.S. protections arise under section 5 of the *Federal Trade Commission Act*, that empower the Federal Trade Commission to take action against organizations for "unfair or deceptive acts or practices in or affecting commerce,"[7] which the FTC has used in cases dealing with organizations' practices with respect to personal information.[8] Under its "deception" authority, the FTC has enforced against entities that make false promises about their information practices, such as in their privacy policies. Alternatively, under its "unfairness" authority, the FTC has brought actions against harmful information practices, but this unfairness authority is limited by a three-part test:

- the act or practice caused or is likely to cause substantial injury to consumers;
- the injury was not outweighed by countervailing benefits to consumers or competition; and
- the injury was not reasonably avoidable by consumers.[9]

Although the FTC's enforcement authorities do provide flexibility in the scope of their mandate to protect consumers against unfair and deceptive acts and practices, and the FCRA already covers the practices of a significant portion of the Big Data industry, the full extent of the Big Data industry in this age of constant data streams and seemingly unlimited potential uses is not explicitly accounted for in the U.S. regulatory scheme. It should also be noted that a number of bills specifically aimed at the data broker industry have been introduced in Congress, though none is passed or is widely anticipated to pass at the time of the writing of this report.

Significantly, all such statutes and bills are limited by the robust notions of freedom of speech which the U.S. Supreme Court has expressly considered to extend to the sale, disclosure and use of data in the particular context of records regarding the prescribing patterns of physicians.[10] This constitutional ruling has indeed empowered data brokers in the United States with the knowledge that efforts to regulate their use of data will face enhanced judicial scrutiny given the data broker's countervailing free speech rights.

Reports, Hearings, and Studies on Data Brokers

The lack of comprehensive oversight of the data broker industry in the United States is not just an observation that has been made by privacy advocates. A 2005 Congressional Research Service Report specifically noted that: "*data brokers are largely free from state legislation.*"[11] The report also noted that concerns with the data broker industry have been in part due to the large amounts of personal information data brokers hold, breaches associated with certain data brokers, and implications for identity theft. The following year, the United States Government Accountability Office (U.S. GAO) issued a report that noted:

> *"Requiring information resellers to take steps to prevent unauthorized access to all of the sensitive personal information they hold would help ensure that explicit data security requirements apply more comprehensively to a class of companies that maintains large amounts of such data. In addition, no federal statute requires companies to disclose breaches of sensitive personal information, although such a requirement could provide incentives to companies to improve data safeguarding and provide consumers at risk of identity theft or other related harm with useful information."*[12]

In 2012, Representatives Edward Markey (D – Massachusetts) and Joe Barton (R-Texas) led a bipartisan Congressional effort and sent letters to nine organizations involved in the commercial trade of information and asked them to identify the scale and scope of their data collection practices, the sources of their data

collection, their business lines, safeguards, and access and correction practices.[13] The letters to the organizations hinted that their practices were not very transparent, suggesting that these organizations have developed *"...hidden dossiers on almost every U.S. customer"*[14] and that the aggregation of all the online and offline data used for marketing purposes can potentially put all Americans, including children, at risk.

The responses received revealed a wide range of activities and data collection practices, which included collecting information from public sources, surveys, product information cards, and, in some cases, purchasing or licensing data from third party sources (such as other data brokers), and gathering information from social network sites. The range of information and categories were broad and deep, involving identifiers such as race and religion and, in some cases, the ranking of individuals for marketing purposes.

As a result, in December 2012, Representatives Markey and Barton, along with the FTC, privacy advocates and several data brokers, held a privacy caucus on the data broker industry.[15] While reports indicate that there was little consensus on how to define data brokers or address concerns about practices, it was notable for being the first ever Congressional hearing on data brokers.[16]

Earlier, in March 2012, the FTC issued a final report[17] on protecting consumer privacy, in which it recommended a more comprehensive privacy framework to improve practices involving the collection and use of consumer information. In addition, the report contained specific recommendations aimed at the data brokerage industry – particularly to increase Big Data transparency. The report builds upon a preliminary report the FTC issued in December 2010.

While the FTC called on Congress to enact baseline privacy legislation, the final report also asked Congress to consider enacting sector specific data broker legislation *"...to provide greater transparency for and control over the practices of information brokers."*[18]

In order to address the lack of transparency with data brokers, the FTC also laid out specific recommendations for the Big Data industry to increase transparency even without legislation. These recommendations included a call for data brokers involved in marketing to create a centralized website to identify themselves to consumers and describe their access to personal information and consumer control choices. These recommendations were intended to promote access and increase the transparency of data brokers' activities.[19]

The FTC privacy framework also recommends that organizations obtain opt-in consent if information is used *"in a materially different manner"* than indicated at the time of collection, or for certain instances involving sensitive data. To facilitate this, the FTC recommended organizations improve and standardize privacy policies. Improving privacy policies is also identified as a means to promote transparency.[20]

Other recommendations included guidance that organizations limit data to what is consistent for the context of a particular transaction, place limits on data retention, take steps to ensure the accuracy of information, and consider third-parties as affiliates unless that relationship is clear to individuals.[21]

The report suggests that the framework should apply to organizations that use data that is linkable to a specific consumer or device. It would not be intended to apply to those organizations that: i) ensure that data is de-identified and are reasonably confident the data cannot be re-identified; ii) publically commit to maintain and use de-identified data; and iii) in cases where de-identified data is made available to other organizations, the organization contractually prohibits re-identification by the other organization.[22]

Given the FTC's enforcement powers, its recommendations are often very persuasive suggestions for data broker practices. And the FTC has followed its report with some enforcement action. In May 2013, after an online enforcement sweep in conjunction with the Global Privacy Enforcement Network (an enforcement collaboration of international data protection authorities organized by the Office of the Privacy Commissioner of Canada), the FTC sent warning letters to 10 data broker companies that their practices could violate the FCRA.[23]

FTC leadership has also continued to raise the profile of these issues. In particular, Commissioner Julie Brill has championed a "Reclaim Your Name" initiative aimed at facilitating more consumer control in Big Data.[24] FTC Chairwoman Edith Ramirez has also been outspoken on these issues, warning data brokers that they must comply with existing data privacy and security regulations and reminding them of the FTC's existing enforcement powers.[25]

In May 2014, the FTC released *"Data Brokers: A Call for Transparency and Accountability."*[26] This report, which followed the FTC's study of nine data brokers, found a lack of transparency in the data broker industry and called for Congress to enact legislation to improve transparency and consumer control. Among other issues, the report found:

- Data brokers collect consumer data from extensive online and offline sources, largely without consumers' knowledge, ranging from consumer purchase data, social media activity, warranty registrations, magazine subscriptions, religious and political affiliations, and other details of consumers' everyday lives.
- Data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences such as those related to ethnicity, income, religion, political leanings, and age. Other potentially sensitive categories include health-related topics or conditions, such as pregnancy, diabetes, and high cholesterol.
- Many of the purposes for which data brokers collect and use data pose risks to consumers, such as unanticipated uses of the data.
- Some data brokers unnecessarily store data about consumers indefinitely, which may create security risks.
- To the extent data brokers currently offer consumers choices about their data, the choices are largely invisible and incomplete.[27]

Given the scope, scale and size of information that data brokers in the United States hold, the merging of offline and online activities, and the sophisticated analytical and technological solutions that exist, data brokers increasingly are compiling mature consumer profiles that paint a more contextual and accurate picture of an individual.

Given the sheer volume of online information and the power of computer analytics, the reality is that information about an individual's online activities can reveal more than just a silhouette. The picture of an individual becomes less opaque and more revealing when offline activities are added to augment profiles, and even sharper details may be brought into focus when this information is derived from a wide range of industries and sectors that an individual interacts with over days, weeks, or even years. The dividing line between personally identifiable information and de-identified data is blurry at best.

C. Canadian Privacy Legislation

There is a distinct difference in the regulatory framework in the United States and in Canada. Unlike in the United States where only certain types of organizations or activities are regulated by specific data protection legislation, the *Personal Information Protection and Electronics Document Act* (PIPEDA) applies to all organizations that collect, use and disclose personal information in the course of commercial activity, except in provinces with substantially similar legislation. PIPEDA still applies to transborder dataflows, and all personal information held by federal works, undertakings and businesses (FWUBs), including information about the employees of FWUBs.

The objective of PIPEDA is to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals and the need of organizations to collect, use and disclose personal information for legitimate business purposes. As a result, PIPEDA creates a balance between the needs of businesses and the privacy rights of individuals.

PIPEDA does not prohibit business practices such as direct marketing, but it does ensure that organizations provide individuals with the opportunity to control the collection, use, and disclosure of their information. Correspondingly, it also requires that those companies that purchase information from data brokers comply with the legislation, to the extent that they too are subject to PIPEDA. By virtue of its scope of application, either alone or in concert with substantially similar legislation, PIPEDA ensures coverage and protection over the broader lifecycle of information by data brokers and third party purchasers.

In this way, PIPEDA, together with substantially similar provincial privacy legislation and public sector privacy legislation have created a privacy landscape much different from that in the United States.

While certain prescribed publically available information may be exempted from consent requirements for collection, use and disclosure, other PIPEDA obligations continue to apply. For example, in a finding from the Office of the Privacy Commissioner of Canada, the Assistant Commissioner found in the case of one organization's practices: *"…while the personal information was publicly available, it nonetheless was still personal information. In order to bring the company in line with the openness principle, she recommended changes to its policies and practices."*[28]

At the time of the writing of this report Bill S-4[29], *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*, had been introduced. Among other issues, the bill proposes to amend PIPEDA to add a new section 7.2 to allow organizations contemplating a "business transaction" to use and disclose personal information without consent subject to certain conditions and safeguards. Subsection 7.2(4) contains a further limit on the use of these provisions. It states that they do not apply in the case of a business transaction "of which the primary purpose or result of the transaction is the purchase, sale or other acquisition or disposition, or lease, of personal information." This would appear to foreclose, for example, a data broker contemplating the purchase of another data broker, from using these provisions.

D. Data Brokers In Canada

The difference in the regulatory environment has been cited as one reason why certain data brokers in the United States do not have operations in Canada, or have modified their business practices in Canada. A research paper funded under the OPC's Contributions Program notes that one American data broker *"...claimed to have stopped dealing with Canadians' personal information after PIPEDA came into force."*[30] The paper also notes that due to Canadian privacy legislation requirements, Canadian data brokers tend to use fewer information sets than in the United States and provide enhanced privacy protections for Canadians.

The paper asserts that the scope and scale of information available in the United States data broker market was greater than in the Canadian market, given that there are more data issued to generate consumer lists, and more information is publically available on Americans than on Canadians.

While the difference between Canadian and U.S. privacy legislation illustrates the differences between organizations' compliance requirements, data brokers can and do operate in Canada. The Contributions Program research paper, while not assessing data brokers' compliance with legislation, does illustrate the wide range of data products, sources and services available. The information below about some Canadian data brokers has been sourced from the paper, and has been updated by reviewing information from the organizations' websites.

Cornerstone Group of Companies (Cornerstone)

According to information from Cornerstone's website,[31] it offers a range of data services, such as managing organizations' consumer lists, marketing solutions, data enhancement solutions, directory services, and geo-demographic and data analytics. Included in this are data cards[32] that provide consumer lists based on a number of different demographic subsets. Research indicates the information is collected from a variety of sources, such as "telephone directories, geodemographic data, direct response data, and scanned listings from third party lists that it manages in-house."[33]

With respect to its data cards, Cornerstone specifically states that the list *"...is subject to and compliant with the Personal Information Protection and Electronic Documents Act."*[34] In addition, its privacy statement notes that it complies with PIPEDA, and takes efforts to ensure that information on lists is collected, used, and disclosed in accordance with PIPEDA.[35]

InfoCanada

InfoCanada layers directory data with information from Statistics Canada, and offers consumer lists, and data analytics solutions. At the time of this report, its website stated that it has information from over 12 million Canadians, and provides demographic categories, such as income range, home type and value, marital status, gender, ethnicity, and religion.[36] Like Cornerstone, its privacy policy states that it complies with PIPEDA, and it maintains that the information they collect from Statistics Canada is not personal information and the directory information is all publically available information.[37]

Credit Bureaus

In Canada, there are two main credit bureaus, Equifax and TransUnion, both of which are subject not only to PIPEDA, but also to provincial consumer credit reporting legislation. Credit bureaus are also involved in the sale of aggregated data for business solutions (such as marketing, risk management, and fraud and identity management) and collect information from public records and credit grantors. In addition, credit bureaus are also increasingly involved in individual authentication activities. Experian used to have operations in Canada, but in 2009 reports indicated that it would be closing its Canadian credit bureau operations due to the global financial environment at the time.[38]

More recently, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) heard that Acxiom has modified its operations in dealing with Canadians. Acxiom appeared before ETHI in December 2012 as part of the Committee's study on social media and privacy. The Committee heard that Acxiom's Canadian operations are limited to "...business and consumer telephone directory products...."[39] It should be noted though that it does append census data to telephone directory information.[40] Furthermore, Acxiom indicated that it does not have plans to expand its Canadian services,[41] and that it screens out Canadian data from any lists that it obtains.[42]

E. Data Brokers In Canada – What Are Potential Privacy Concerns?

When looking at potential concerns related to organizations that trade in information, issues such as Big Data, the risks associated with safeguarding large amounts of personal information, and the associated implications of a data breach are relevant in an age where storing and compiling data have become easier and cheaper. The additional challenge in today's world of sophisticated analytical technological solutions is that these solutions, in combination with Big Data and the rich and contextual profiles that data brokers hold, should be taken into account to responsibly determine the risk of re-identification.

Another dimension to Big Data is its use for knowledge discovery through the application of data mining techniques. Knowledge discovery, as its name implies, uncovers new knowledge that was not known previously. Where such discovery involves information about a person, and that information is used for a purpose not previously identified and without consent, privacy issues arise. Knowledge discovery can be highly problematic due to the fact that the person himself or herself may not know that the information exists, let alone that it is being analyzed and used by others. A simple example is "Alice always buys a car on even years when the moon is closest to the earth." Here, Alice herself may not realize that she has this habit, or that this information is being used to profile or target her.

The use of apparently anonymized or aggregated data may, on the surface, seem to fall outside the scope of PIPEDA since by definition anonymous data do not qualify as personal information under the Act.[43] The OPC has however tended to take a contextual approach to assessing what is personal information.[44] The courts have also found that information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.[45] That said, there does remain the possibility that customer lists could be anonymized and made available for sale. While this practice does still need to be made clear by organizations in their privacy policies, the re-identification risk of anonymized data is an ongoing concern.

In a paper by El Emam and Kosseim,[46] it was noted that re-identification risk (in the context of retail and hospital pharmacy data released to data brokers), is real and depends on several variables, including how much information is released, and how "motivated" an intruder is. As such, it cannot be presumed that anonymized data will remain anonymous.

In addition, the use of cloud computing raises concerns about data brokers' ability to demonstrate accountability, safeguard information, and manage risks associated with transborder dataflows and foreign jurisdiction access. Managing multiple copies of records, especially in addressing the accuracy of information, access requests and complaints can also be challenging.

Finally, the interconnected nature of the digital economy has increased the reach of organizations outside of Canada. While compliance with PIPEDA is required in cases where there is a real and substantial link to Canada, the extent to which organizations outside of Canada know of, adhere to, and meet those obligations - or wilfully disregard them - remains largely unknown.

The above risks, while not unique to the data broker industry, are more complex and can have a greater impact on the privacy of Canadians than other sectors, given the scope, scale, and nature of data broker business lines.

F. Conclusion

The online and digital environment has fundamentally changed how individuals and business communicate. Online and digital platforms have challenged not only the manner in which communication takes place, but have also allowed some data brokers to meld the offline and online worlds to create mature and contextual profiles of individuals.

The data broker industry in Canada operates under a comprehensive privacy and regulatory compliance framework that is distinct from the situation in the United States. Nonetheless, the challenges associated with emerging privacy trends and issues means that privacy remains an ever important concept in balancing the legitimate commercial needs against the privacy rights of Canadians.

As well, in an interconnected digital economy, borders are easily crossed and access to personal information has never been easier. Whether data brokers based in other jurisdictions know of PIPEDA and comply with its requirements when doing business in Canada remains an open question. Hence the ongoing need to make PIPEDA requirements and expectations known to data broker organizations on either side of the border that are interested in doing business in Canada.

Endnotes

[1] As read in Canadian Internet Policy and Public Interest Clinic, *"On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship,"* 2006, pg.2. Online at: http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Referenced from Footnote 3 from Daniel Solove, *"The Digital Person: Technology and Privacy in the Information Age,"* New York University Press.

[2] David Leduc, *"Data Broker Briefing Reveals Complex Data Ecosystem,"* The Software & Information Industry Association, December 18, 2012. Online at: http://www.siia.net/blog/index.php/2012/12/data-broker-briefing-reveals-complex-data-ecosystem/

[3] David Leduc, "Data Broker Briefing Reveals Complex Data Ecosystem," The Software & Information Industry Association, December 18, 2012. Online at: http://www.siia.net/blog/index.php/2012/12/data-broker-briefing-reveals-complex-data-ecosystem/

[4] The Federal Trade Commission, "*FTC to Study Data Broker Industry's Collection and Use of Consumer Data."* News release, December 18, 2012. Online at: http://www.ftc.gov/opa/2012/12/databrokers.shtm

[5] For example, The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. The United States Senate, Committee on Commerce, Science, and Transportation. Letter to Acxiom, May 9, 2012. Online at: http://commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c. Representatives Edward Markey (D- Massachusetts) and Joe Barton (R-Texas) letter to 9 Data Brokers, July 24, 2012. Online at: http://markey.house.gov/content/letters-major-data-brokers. This link is no longer available, but can be accessed at: http://web.archive.org/web/20120730010134/http://markey.house.gov/content/letters-major-data-brokers. The Federal Trade Commission announcement of a study of data brokers and orders sent to data brokers, December 2012. Online at: http://www.ftc.gov/opa/2012/12/databrokers.shtm

[6] Maeve Z. Miller, *"Why Europe Is Safe From ChoicePoint: Preventing Commercialized Identity Theft Through Strong Data Protection And Privacy Laws,"* The George Washington International Review, vol 39, 2007, pgs. 402-403.

[7] 15 U.S.C. § 45(a)(1); see also Daniel J. Solove & Paul Schwartz, Privacy Law Fundamentals 2013, at 137-38 (2013) (breaking down FTC actions). Each state also has its only "little FTC Act" enforced by its state Attorney General.

[8] The Federal trade Commission, Resources for Reporters - Making Sure Companies Keep Their Privacy Promises to Consumers. Online at: http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml

[9] 15 U.S.C. § 45(n); FTC v. NHS Sys., Inc., No. 08-2215, 2013 WL 1285424, at *5 (E.D. Pa. Mar. 28, 2013). "[T]he consumer injury test is the most precise definition of unfairness articulated by either the Commission or Congress." Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985) (rejecting argument that "the FTC has no authority to proscribe the 'kinds' of practices or prevent the 'kinds' of consumer injury at issue in this case").

[10] *Sorrell v. IMS Health Inc.*, 131 S.Ct. 2653 (2011).

[11] Nathan Brooks, *"Data Brokers: Background, Industry and Overview,"* Congressional Research Service, The Library Of Congress, Order Code RS 221377, May 2005, pg. 1. Online at: http://assets.opencrs.com/rpts/RS22137_20050505.pdf.

[12] Government Accountability Office, *"GAO-06-674, a report to the Committee on Banking, Housing and Urban Affairs, U.S. Senate: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data," June 2006. Online at:* http://www.gao.gov/assets/260/250627.html

[13] Representatives Edward Markey (D- Massachusetts) and Joe Barton (R-Texas) letter to 9 Data Brokers, July 24, 2012. Online at: http://markey.house.gov/content/letters-major-data-brokers. This link is no longer available, but can be accessed at: http://web.archive.org/web/20120730010134/http://markey.house.gov/content/letters-major-data-brokers

[14] Representatives Edward Markey (D- Massachusetts) and Joe Barton (R-Texas) letter to 9 Data Brokers, July 24, 2012. Online at: http://markey.house.gov/content/letters-major-data-brokers. This link is no longer available, but can be accessed at: http://web.archive.org/web/20120730010134/http://markey.house.gov/content/letters-major-data-brokers

[15] Representative Edward Markey (D- Massachusetts) website, News webpage, December 12, 2012. Online at: http://markey.house.gov/press-release/markey-barton-ftc-study-data-brokers. This link is no longer available, but can be accessed at: http://web.archive.org/web/20130220162934/http://markey.house.gov/press-release/markey-barton-ftc-study-data-brokers

[16] Alston and Bird LLP, Alston's Privacy + Security Blog, *"Congressional Bi-Partisan Privacy Caucus Holds Roundtable Briefing on Data Broker Practices,"* December 14, 2012. Online at: http://www.alstonprivacy.com/?entry=4765

[17] The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[18] The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, pg. iv. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[19] The information from this paragraph is taken from The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, pgs. viii. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[20] The information from this paragraph is taken from The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, pgs. viii. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

[21] The information from this paragraph is taken from The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012. Pgs. 26-41. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf
[22] The Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, pg. iv. Online at: http://www.ftc.gov/os/2012/03/120326privacyreport.pdf
[23] FTC Warns Data Broker Operations of Possible Privacy Violations: Letters Issued as Part of Global Privacy Protection Effort , May 7, 2013. Online at: http://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations
[24] Federal Trade Commission Commissioner Julie Brill, Reclaim Your Name: Keynote Address by Commissioner Julie Brill, 23rd Computers Freedom and Privacy Conference, June 26, 2013. Online at http://www.ftc.gov/public-statements/2013/06/reclaim-your-name.
[25] Federal Trade Commission Chairwoman Edith Ramirez, The Privacy Challenges of Big Data, A View from the Lifeguard's Chair, August 19, 2013. Online at http://www.ftc.gov/public-statements/2013/08/privacy-challenges-big-data-view-lifeguard's-chair.
[26] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 27th, 2014. Online at: http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf
[27] FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information, May 27th, 2014. Online at: http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more
[28] Office of the Privacy Commissioner of Canada: PIPEDA Case Summary #2009-004: No Consent Required for Using Publicly Available Personal Information Matched with Geographically Specific Demographic Statistics. Online at: http://www.priv.gc.ca/cf-dc/2009/2009_004_0109_e.asp
[29] Please see An Act to amend the Personal Information Protection and Electronic Documents Act
[30] Canadian Internet Policy and Public Interest Clinic, "*On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship,*" 2006, pg.45. Online at: http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf
[31] This information was obtained from referring to the Cornerstone Group Of Companies website. Online at: http://www.cstonecanada.com/
[32] Data cards include the list name, data selects, update frequency, recommended usage, and other relevant information for potential purchasers. As noted in Canadian Internet Policy and Public Interest Clinic, "*On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship,*" 2006, pg.12. Online at: http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf
[33] Canadian Internet Policy and Public Interest Clinic, "*On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship,*" 2006, pg.19. Online at: http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf
[34] A sample search was done on the data cards from Cornerstone Group of Companies' website using the topic of CANADIAN FAMILY for the data card search. This search led to online at: http://www.cstonecanada.com/datacards/datacard.aspx?uid=65a701dd-9efa-4d32-a68c-38cb163c0036
[35]Cornerstone Group of Companies Website – Privacy Policy. Online at: http://www.cstonecanada.com/privacy/index.asp
[36] This information was obtained from referring to InfoCanada's website. Online at: http://www.infocanada.ca/main_page.aspx
[37]This information was obtained from referring to InfoCanada's website - Privacy Policies. Online at: http://www.infocanada.ca/privacy.aspx?bas_session=S688251728274 31&bas_vendor=99911
[38] Tom Drake, *"Experian Closes Their Canadian Consumer Credit Bureau,"* Canadianfinanceblog, Online at: http://canadianfinanceblog.com/experian-closes-their-canadian-consumer-credit-bureau/
[39] 41st Parliament, 1st Session, Standing Committee on Access to Information, Privacy and Ethics, Evidence, Thursday, December 6, 2012, Study on Social Media and Privacy. Testimony By Ms. Jennifer Barrett Glasgow, Global Privacy and Public Policy Executive, Acxiom, At (1635). Online at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5927254#Int-7842856
[40] 41st Parliament, 1st Session, Standing Committee on Access to Information, Privacy and Ethics, Evidence, Thursday, December 6, 2012, Study on Social Media and Privacy. Testimony By Ms. Jennifer Barrett Glasgow, Global Privacy and Public Policy Executive, Acxiom, At (1635). Online at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5927254#Int-7842856
[41] 41st Parliament, 1st Session, Standing Committee on Access to Information, Privacy and Ethics, Evidence, Thursday, December 6, 2012, Study on Social Media and Privacy. Testimony By Ms. Jennifer Barrett Glasgow, Global Privacy and Public Policy Executive, Acxiom, At (1640). Online at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5927254#Int-7842856

[42] 41st Parliament, 1st Session, Standing Committee on Access to Information, Privacy and Ethics, Evidence, Thursday, December 6, 2012, Study on Social Media and Privacy. Testimony By Ms. Jennifer Barrett Glasgow, Global Privacy and Public Policy Executive, Acxiom, At (1655). Online at: http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5927254#Int-7842856

[43] Teresa Scassa, *"Privacy and Open Government,"* (2014) 6. *Future Internet*, 397-413. Online at: http://www.mdpi.com/1999-5903/6/2/397; and Teresa Scassa, *"Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy,"* (2009) 7:2. Canadian Journal of Law and Technology 193-222. Online at: http://www.teresascassa.ca/Files/publications/scassa_1.pdf

[44] The Office of the Privacy Commissioner of Canada, *"Report on the 2010 Office of the Privacy Commissioner of Canada's Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing"* 2012. Online at: http://www.priv.gc.ca/resource/consultations/report_201105_e.asp

[45] Gordon v. Canada (Health), 2008 FC 258 (CanLII). Online at: http://www.canlii.org/en/ca/fct/doc/2008/2008fc258/2008fc258.htm

[46] Khaled El Emam, Patricia Kosseim *"Privacy Interests in Prescription Data, Part 2: Patient Privacy,"* IEEE Security & Privacy 7(2): 75-78 (2009). Online at: http://www.computer.org/csdl/mags/sp/2009/02/msp2009020075-abs.html