

Monetizing Data: Seizing Opportunities, Managing Risk

September 28, 2016

Arun Bauri, Strategic Policy and Research Analyst, Office of the Privacy
Commissioner of Canada

Kirsten Thompson, Partner, McCarthy Tétrault

Donald Houston, Partner, McCarthy Tétrault



Agenda

1. Overview

2. Privacy and Consent in Data Monetization

- Arun Bauri (Strategic Policy and Research Analyst, Office of the Privacy Commissioner of Canada)

3. Competition Law Issues in Data Monetization

- Don Houston (Partner, McCarthy Tétrault)

4. Strategies for Managing Legal Risk

- Kirsten Thompson (Partner, McCarthy Tétrault)

Overview of Data Monetization



Overview

- **Big Data:** large volumes of high velocity, complex, and variable data requiring advanced techniques and technologies to enable capture, storage, distribution, management, and analysis

CHARACTERISTIC	DESCRIPTION
Volume	The sheer amount of data generated or data intensity that must be ingested, analyzed, and managed to make decisions based on complete data analysis
Velocity	How fast data is being produced and changed and the speed with which data must be received, understood, and processed
Variety	The rise of information coming from new sources both inside and outside the walls of the enterprise or organization creates integration, management, governance, and architectural pressures on IT

Overview

- **Data monetization:** generation of revenue from available data sources or streamed data via discovery, capture, storage, analysis, dissemination, and use of that data
- The Internet of Things generates location data and other data from sensors and devices at an ever increasing rate
- When this data is collated against traditional databases, the value and utility of both sources of data increases

Overview

- Data monetization can be about selling data directly:
 - Bartering or trading with information
 - Information-enhanced products or services
 - Selling raw data through brokers
 - Offering data/report subscriptions
- Most of the time, monetization is less direct: making a process run more efficiently, incentivizing certain types of behavior, or revealing the true value of an asset

Overview

- Five basic models make up the spectrum of activity for transforming your approach to information:
 - Current core business, improved through use of enhanced data
 - Better return on marketing investment using insights (customers or transactions)
 - White-label capabilities and infrastructure delivered by other firms
 - Delivery of new types of data directly to customers
 - New products and services made possible by data and analytics

Less Transformative



More Transformative

Overview

- In order to effectively assist your organization navigate the risks associated with monetization, you need to know how it uses data now and how it plans to use data in the future
- Some of the risks:
 - Regulatory risk
 - Contractual risk
 - Liability risk
 - Insurance risk
 - Consumer relationship risk

Privacy and Consent in Data Monetization



Monetizing Data – Seizing Opportunities, Managing Risk

*Presentation: McCarthy Tétrault
September 28th 2016*



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada



OPC Role and Mandate

- Oversee compliance with:
 - *Privacy Act*
 - *Personal Information Protection and Electronic Documents Act (PIPEDA)*
- Purpose of PIPEDA:

“...recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.”



OPC Strategic Privacy Priorities

Vision: Canadians will have greater control over their personal information

Priorities	ECONOMICS OF PERSONAL INFORMATION	GOVERNMENT SURVEILLANCE	REPUTATION & PRIVACY	THE BODY AS INFORMATION
Goals	<i>The OPC will have enhanced the privacy protection and trust of individuals so that they may confidently participate in an innovative digital economy.</i>	<i>The OPC will have contributed to the adoption and implementation of laws that demonstrably protect both national security and privacy.</i>	<i>The OPC will have helped to create an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.</i>	<i>The OPC will have promoted respect for the privacy and integrity of the human body as the vessel of our most intimate personal information.</i>
Strategies for achieving our goals	Exploring innovative and technological ways of protecting privacy			
	Strengthening accountability and promoting good privacy governance			
	Protecting Canadians' privacy in a borderless world			
	Enhancing our public education role			
	Enhancing privacy protection for vulnerable groups			



Economics of Personal Information

- A first goal for the OPC will be to enhance the privacy protection and trust of individuals so that they may confidently participate in an innovative digital economy
- Personal information/data plays a large role for monetization in the digital economy
- Complexity in digital environment business models and technologies raises questions with consent



Consent Discussion Paper

- Identify and explore potential enhancements to the consent model
- Provide an overview of the landscape, key issues and potential solutions to stimulate dialogue
- Under PIPEDA: “...the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting”



Consent Discussion Paper

- Challenges to the Consent Model:
 - New technologies and business models
 - Big Data
 - Internet of Things (IoT)
 - Human Behaviour



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Consent Discussion Paper: Possible Solutions

- Enhancing Consent
- Alternatives to Consent
- Governance
- Enforcement Models



Consent Paper: Discussion Questions

- Of the solutions identified in this paper, which one(s) has/have the most merit and why?
- What solutions have we not identified that would be helpful in addressing consent challenges and why?
- What roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effective system?
- What, if any, legislative changes are required?



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Next Steps

- Cross-Canada Meetings
 - Broad range of stakeholders
- In parallel: OPC paper on reputation



Key Takeaways

- Just as monetization requires cross-enterprise approach the same approach needs to be given to the related privacy considerations
- Innovative ways to engage individuals in the digital economy are enhanced with:
 - Innovative ways with communicating privacy information
 - Leveraging privacy-sensitive practices as part of the monetization strategy
 - Creating a culture where a proactive approach to privacy protection fosters trust on the part of individuals that their data will not be used in unanticipated ways and without their consent



Key Takeaways

- Monetization of data strategies are broader than looking at business model and consumer engagement strategies:
 - Accountability - Privacy Management Program/Training/Policies and Procedures
 - Risk Mitigation - Threat Risk Assessment/Privacy Impact Assessment
 - Privacy by Design/Privacy by Default from the outset
 - Transparency and openness can help demystify seemingly invisible practices
 - Consent and control can mitigate concerns where there are complex partnerships and data flows
 - Schedule 1 of PIPEDA



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

www.priv.gc.ca

@privacyprivee

1-800-282-1376

Competition Law Issues in Data Monetization



MONETIZING DATA – COMPETITION ISSUES

“The collection, analysis and use of data is increasingly becoming an important source of competition advantage in the digital economy, driving innovation and product improvement.”
[Competition Bureau (Canada), April 19, 2016]

MONETIZING DATA – COMPETITION ISSUES

“If data can help you compete, by improving your services and cutting costs, then having the right set of data could make it almost impossible for anyone else to keep up. So we need to be sure that companies which control that sort of data don't use it to stop others from competing.”
(Margrethe Vestager, EC Competition Commissioner, September 9, 2016)

MONETIZING DATA – COMPETITION ISSUES

“Data-driven companies play an important and growing role in Canada’s economy. We will continue to monitor firms in the digital economy to ensure they do not engage in anti-competitive conduct.” (John Pecman, Commissioner of Competition, Canada)

COMPETITION ISSUES - INTRODUCTION

- Competitive laws focus on market power.
- Market Power: "...the ability to profitably influence price, quality, variety, service, innovation or other dimensions of competition."
- Where collection, analysis or use of data creates or enhances market power, competition laws may be engaged.
- Privacy issues are not part of competition law, but can be relevant in competition context.
- Potential for conflict between competition and privacy (e.g. TREB)

Relevant Competition Act Provisions

- **Mergers (S.92)** – Mergers which are likely to substantially lessen or prevent competition may be challenged before the Competition Tribunal.
 - Where combining data held by merging parties could create or enhance market power, competition authorities may intervene.
 - e.g. – Google/DoubleClick, EC, 2008
 - e.g. – Facebook/Whatsapp, EC, 2014
 - In both cases, EC looked at whether combining data would enhance market power, and concluded it would not.

Relevant Competition Act Provisions

- **Abuse of dominance (S.79)** – Where a company with a **dominant market position** engages in a **practice of anti-competitive acts** which is likely to result in a **substantial lessening or prevention of competition**, it may be subject to prohibition order and AMP.
e.g. – D & B Companies (1995)
e.g. – TREB (ongoing)

Relevant Competition Act Provisions

- **Conspiracy (S. 45)** – Agreements by competitors to fix the prices of the products or services they sell are criminal offences.
 - Sharing of competitively sensitive data among competitors can lead to inferences of collusion/conspiracy.
 - Increased transparency of certain data (e.g. prices) can also lead to inferences of collusion/conspiracy.
 - See *United States v. Airline Tariff Publishing Co. et al.*, 836 F. Supp. 9 (U.S.D.C. 1993)
- Also potential for civil review (**S.90.1**)

CANADIAN CASE EXAMPLES

- *Canada (DIR) v. D & B Companies of Canada Ltd. (1995), 64 C.P.R. (3d) 216 (Comp. Trib.)*
 - Abuse of dominance case.
 - Respondent found to be dominant supplier of “scanner-based market tracking services” in Canada.
 - Respondent found to have engaged in practice of anti-competitive acts by entering into contracts with all major grocery retailers for exclusive access to their scanner data.
 - Conduct found to result in substantial lessening and prevention of competition by precluding entry of other providers of scanner-based market tracking services.
 - Tribunal prohibited respondent from enforcing exclusivity terms and from entering into further exclusive contracts for scanner data.

CANADIAN CASE EXAMPLES

- *Commissioner v. Toronto Real Estate Board (TREB) 2016 Comp. Trib. 8*
 - Abuse of dominance case.
 - Relevant Market: Supply of MLS-based residential real estate brokerage services in the GTA.
 - Industry association (TREB) found to have market dominance through its control of MLS system and data.
 - Rules passed by TREB restricted ability of internet-based brokerages to post of certain MLS data on their websites.

Toronto Real Estate Board (TREB) case continued

- Data in question limited to sold data, expired listings, commission info.
- Rules found to be practice of anti-competitive acts.
- Tribunal rejected TREB claims that restrictions were based on privacy considerations.
- Tribunal focused on TREB motivation/purpose, less on objective third party privacy interests.
- Tribunal found that restrictions lessened and prevented competition by stifling innovation from internet-based real estate brokerages.
- TREB ordered to remove restrictions on the disputed data and to pay Commissioner's costs (\$1.8million).

Toronto Real Estate Board (TREB) case continued

- TREB has appealed to FCA.
- FCA recently granted stay of Tribunal Order pending appeal and ordered expedited appeal.
- Stay based on privacy considerations:
“...I believe there to be a non-frivolous argument that the Tribunal did not fully consider all of the relevant impacts of its orders on third party privacy interests...” (Gleason, J.A, August 12, 2016)

Competition Bureau Investigation Of Google (2013-2016)

- **2013-2016** – Bureau investigated allegations of abuse of dominance regarding Google's online search and search advertising services in Canada.
- Bureau concluded that Google possessed market power in markets for online search and search advertising services in Canada.
- Bureau found certain terms in Google's API agreements to be anti-competitive. Google had committed to FTC to change this, gave same commitment to Bureau.
- Bureau found other allegations not substantiated, so discontinued investigation in 2016.
- But Bureau committed to “continue actively monitoring the digital marketplace.

Strategies for Managing Legal Risk



Strategies for Managing Risk

- Know your **industry/sector**:
 - Banks:
 - Banks can only carry on the “business of banking and such business as generally appertains thereto” subject to certain specific exceptions (s. 409 *Bank Act*)
 - In particular, banks cannot engage in any trade or other business (s. 410(2) *Information Technology Activities (Banks) Regulations*)
 - Insurance Companies:
 - Similarly, federal trust companies and insurance companies can only carry on such business generally as appertains to the business of providing financial services (s. 440 *Insurance Companies Act*, s. 409 *Trust and Loan Companies Act*)

Strategies for Managing Risk

→ Auto Insurance:

→ Usage-based auto insurance pricing (“UBIP”), FSCO Bulletin No. A-05/13:

- “Any personal information collected through a UBIP program, or its accompanying devices or software, should not be disclosed to any other party unless expressly consented to by the person...”
- “Drivers should be able to enroll in a UBIP program without being required to share their personal information for non-UBIP purposes (e.g., marketing, offering of additional services such as vehicle location services or assistance in emergency situations).”
- “UBIP programs [...] should collect and use UBIP data solely for discount-setting purposes, and not to decline, cancel or refuse to renew risks or to confirm rating criteria currently used...”
- “Insurers should [...] facilitate drivers using their personal UBIP data for the purposes of entering into a contract with another insurer including enrolling in another insurer’s UBIP program.”

Strategies for Managing Risk

- Know your **existing ecosystem**:
 - Privacy
 - CASL/Do Not Call
 - Consumer protection
 - Health
 - Labour
 - Human Rights Act
 - Criminal Code

Strategies for Managing Risk

- Know your **evolving ecosystem**:
 - Privacy
 - Pending regulations for recordkeeping, breach reporting
 - CASL
 - Private right of action July 2017
 - Health
 - Bill S-201 - *Genetic Non-Discrimination Act*: An Act to prohibit and prevent genetic discrimination
 - Second reading (House), as of Sept. 20, 2016

Strategies for Managing Risk

→ Know your **data**:

- Is it personal information? Could it become personal information? Sensitive personal information? (*PIPEDA Report of Findings #2015-001 (Bell RAP)*)
- Even with consent, use must be “appropriate” (*s 5(3) PIPEDA*)
- “...the practice of using [loyalty plan] members' information for purposes of advertising products, services, and special promotions remains unobjectionable in itself, [however] a reasonable person would not expect such practice to extend to the "tailoring" of information to the individual's potentially sensitive personal or professional interests, uses of or preferences for certain products and services, and financial status, without the positive consent of the individual.” (*PIPEDA Case Summary #2002-42*)

Strategies for Managing Risk

- The personal information was part of a business transaction, so you don't need consent?
 - True...but not if “the primary purpose or result is the purchase, sale or other acquisition or disposition, or lease, of personal information” (s 7.2(4) PIPEDA)
- How will you manage a request to remove or correct?

Strategies for Managing Risk

- Where did it come from?
 - Open data: OpenCanada.ca, @Open_TO
 - Closed data: data under contract or licence
- Closed data:
 - non-disclosure agreements, confidentiality clauses
 - compilation in databases or websites to which only registered members/customers can access
 - use of a proprietary or closed technology or encryption which creates a barrier for access e.g. “screen scraping” technologies
 - copyright forbidding re-use of the data, including the use of “no derivatives” requirements (also, database rights)
 - restriction of robots to websites, with preference to certain search engines

Strategies for Managing Risk

- Know your **contracts**:
 - What are your reps and warranties? What are theirs?
 - How broad is your indemnification?
 - Is there a cooperation clause in respect of data incidents/breaches?
 - Breach notifications?
 - De-identification prohibition?
- Loyalty programs, payment cards, digital marketing agreements

Strategies for Managing Risk

- Know your **process**:
 - If you are providing data/personal information, how are you doing so?
 - Aggregate anonymized data?
 - Consent?
 - Open APIs?
 - Cybersecurity, data standards?
 - Has your privacy policy kept pace with your uses/purposes?
 - Who is doing the data crunching?

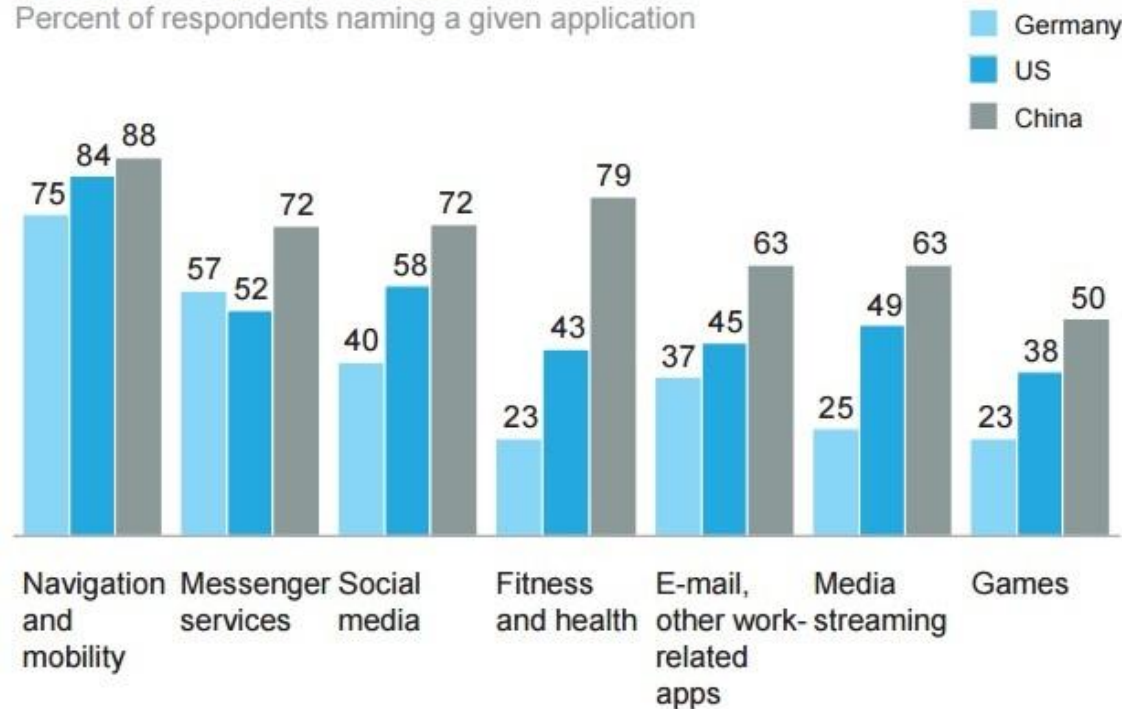
Strategies for Managing Risk

→ Know your **customers/clients**:

Customers across investigated geographies are willing to share navigation data, with visible regional differences in willingness to share other data

If you were to receive an application for free instead of paying for it, would you agree that the application could use your personal data in return? If so, which application would you grant access?

Percent of respondents naming a given application



Higher willingness to share data for navigation and mobility possibly driven by customers' **higher familiarity** and better **understanding of what they get** in ex-change for their data – significantly lower willingness for other applications that are less clear to customers!

SOURCE: McKinsey Connectivity and Autonomous Driving Consumer Survey, 2015

Strategies for Managing Risk

- Consumer attitudes vary according to the type of data
 - 9/10 people consider financial data and data regarding payment card use private
 - 7/10 think that information about children, spouses, health status, and telephone communications is inherently private
 - Consumers are somewhat less sensitive about the privacy of their location, Internet use, e-mail, purchasing history, and use of social networks, although half of consumers consider such data private as well

Source: BCG Global Consumer Sentiment Survey 2013 (EU)

Strategies for Managing Risk

→ Consumer trust matters:

“It is certainly in [companies’] interest to find new ways to inform consumers, meaningfully yet effectively, so as to maintain trust. But will they be up to the challenge? And even if they want to, can they, given that they may not be impartial? [...] Consumer trust and effective privacy protection demands the intervention of regulators that are capable of holding organizations to account and protecting the interests of individuals.”

- *Address by Daniel Therrien, Privacy Commissioner of Canada at the Privacy Laws and Business International Conference, Cambridge, UK (July 5, 2016)*

Strategies for Managing Risk

- PIPEDA Report of Findings #2016-005 (Ashley Madison)
 - False or misleading statements may impact the validity of consent
 - e.g. about security safeguards, practices
 - Omission or lack of clarity of material statements may also impact the validity of consent
 - e.g. retention practices

Strategies for Managing Risk

- Conversely, don't know your customers: anonymization and aggregation
 - **EU Directive:** all the means “likely reasonably to be used either by the data controller or by any other person” to identify an individual must be taken into consideration to determine if the data is anonymous
 - **G29:** if, after taking into account all the means of anonymization, the possibility of identifying a person does not exist or is negligible, the person should not be considered as identifiable
 - **CNIL (France):** data controller must examine whether it is theoretically possible (even if highly improbable) that an individual can be directly or indirectly identified using other data or means anywhere in the world.
 - **Canada (federal):** Personal information that has been de-identified does not qualify as anonymous information if there is a serious possibility of linking the de-identified data back to an identifiable individual (*PIPEDA Case Summary #2009-018*)

Questions?



CPD Information:

This program qualifies for up to 1.5 hour(s) of eligible educational activity or CPD/MCE credit under the mandatory education regimes in British Columbia, Ontario and Québec.

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5
Tel: 604-643-7100
Fax: 604-643-7900
Toll-Free: 1-877-244-7711

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500
Fax: 403-260-3501
Toll-Free: 1-877-244-7711

TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON M5K 1E6
Tel: 416-362-1812
Fax: 416-868-0673
Toll-Free: 1-877-244-7711

MONTRÉAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2
Tel: 514-397-4100
Fax: 514-875-6246
Toll-Free: 1-877-244-7711

QUEBEC

500, Grande Allée Est, 9e étage
Québec QC G1R 2J7
Tel: 418-521-3000
Fax: 418-521-3099
Toll-Free: 1-877-244-7711

UNITED KINGDOM AND EUROPE

125 Old Broad Street, 26th Floor
London EC2N 1AR
UNITED KINGDOM
Tel: +44 (0)20 7786 5700
Fax: +44 (0)20 7786 5702

