Some Privacy Implications of Digital Advertising

fogler rubinoff

Presentation to
Lexpert's 8th Annual Information Privacy and Data Protection Conference
by Bill Hearn, Partner, Fogler Rubinoff, LLP
December 1, 2016, Toronto

fogler rubinoff

Overview

- How has digital advertising been changed by the Internet of Things (**IoT**) and Big Data (**BD**)?
- What are the main privacy law compliance challenges raised by these now prevalent innovative data technologies?
- What are privacy regulators in the EU, US and Canada doing to address these challenges?

fogler rubinoff

Overview

- How can consent under privacy law be made more meaningful while not stifling innovation and growth?
  - How can consent be enhanced?
  - What are the alternatives where consent is not practicable?
  - What else can be done?

fogler rubinoff

What's the IoT?

- Arises from a confluence of existing technologies – sensors, cheap computational power & storage, and ubiquitous interconnection & data
- A term that describes the ability of everyday things (that do not fit the traditional concept of a computer) to communicate with each other using embedded sensors that are linked through the Internet
- These things include "smart" home devices (like thermostats, smoke alarms, security systems, washing machines, TVs, fridges and light bulbs), connected cars and fitness trackers, to name a few

fogler rubinoff

What's the IoT?

- These interconnected devices use the Internet to transmit, compile and analyze data
- Unlike computers and mobile phones, many IoT devices do not have keyboards or screens making it difficult, if not impossible, for the user to know what the device is doing, let alone consent to what is being done

fogler rubinoff

What's the IoT?

OPC's IoT Paper – February 2016

- IoT devices have become part of everyday life and consumer products
- The collection of IoT information is driven by a desire to understand individuals' activities, movements and preferences, and inferences can be drawn about individuals
- To many organizations, the value lies not in the revenue from selling IoT devices but in the data that is generated and processed through BD algorithms

fogler rubinoff

What's the IoT?

OPC's IoT Paper – February 2016

- Data collection and sharing in the IoT environment is often invisible to individuals; it is done device-to-device, without human involvement, as a result of routine activities
- A key challenge is how to convey meaningful information about privacy risks in order to inform the user's decision whether or not to provide consent

fogler rubinoff

What's the IoT?

OPC's IoT Paper – February 2016

- The ubiquitous collection of data and the potential for unexpected uses of data are two serious privacy risks of IoT
- Much of this data is sensitive or rendered sensitive by combining data from different sources
- The data may also be used beyond consumers' reasonable expectations

fogler rubinoff

What's BD?

- BD refers to data sets so large or complex that traditional data processing applications are inadequate
- Challenges include analysis, capture, data curation, search, sharing, storage, visualization and protecting privacy
- BD is a term that describes large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management and analysis of the information

fogler rubinoff

What's BD?

- BD refers to collecting, analysing and generating insights from a wide variety of customer, commercial and environmental information
- BD is used to develop a better understanding of customer preferences, habits and considerations in making transactions with different categories, brands and channels
- The successful use of BD in advertising and marketing leads to improved customer experience, a better exchange of value between customers and organizations, and improved business performance

fogler rubinoff

What's BD?

- Some see the confluence of BD and digital marketing as the "Holy Grail" of advertising and marketing
- BD and mobile allows advertisers and marketers to target customers precisely and efficiently with highly relevant offers tailored to the customer's attributes delivered at the right time and place
- But privacy concerns loom large

fogler rubinoff

Some Privacy Concerns

Identifying Purposes/Knowledge, Consent

- The complexity of the IoT and BD ecosystem and the practical limitations of privacy notices and policies may make it a challenge for individuals to understand what will happen to their personal information (**PI**) – e.g., PI may end up in the database of a data broker and combined and disclosed in ways not easily understood by the individual even if disclosed in privacy notices and policies

fogler rubinoff

Some Privacy Concerns

Identifying Purposes/Knowledge, Consent

- The individual may simply not understand where their PI may end up, and that it could be combined with other existing profile data in a manner that reveals more than contemplated at the time of disclosure
- Onward transfer and combining with yet more data could reveal even more and compound the problem
- The individual data subject may lack an understanding of the interpretations, inferences and deductions that may be drawn from their combined data using BD mining techniques and analytics
- Hence, the “notice and consent” pillars of PIPEDA are being challenged

fogler rubinoff

Some Privacy Concerns

Openness, Accuracy, Individual Access

- Individuals may not know what entities may be collecting information about them and creating profiles
- Data subjects may be able to identify companies to whom they have provided PI and may have a direct relationship with those companies … but they may not be able to do the same for data brokers
- Even if the individual can identify a data broker, they may have challenges getting access to their PI for correction and ensuring accuracy

fogler rubinoff

Some Privacy Concerns

De-identification and Re-identification

- Data sets that are de-identified have had key information stripped away in order to prevent others from identifying the individuals to whom the data set relates
- But if de-identification is not performed properly, it may be possible to re-identify individuals in an anonymized data set
- The risk of re-identification of BD sets using contextual “micro data” is a significant privacy concern (as this may constitute a data breach and attract regulatory investigations and lawsuits)

fogler rubinoff

What's the EU Doing?

- Taken from OPC's Consent Paper May 2016
- Current - Article 6 of EU Data Protection Directive
  - Consent is one of six legal grounds on which personal data can be processed
  - Personal data may also be processed to support the data controller's legitimate interests provided they are not overridden by the fundamental rights and freedoms of the data subject

fogler rubinoff

What's the EU Doing?

- Proposed - General Data Protection Regulation
  - Will replace EU Directive (likely in 2018)
  - Seems to make more stringent the consent requirement – i.e., consent must be freely given, specific, informed and unambiguous; it must be expressed through a statement or another clear affirmative action, such as ticking a box on a website; and silence or inactivity may not constitute consent
  - But also keeps the "legitimate interest" provision – that is, businesses will not need to rely on consent if they can prove that the data processing is necessary for the legitimate interests of the business ... again, except where such interests are overridden by the fundamental rights and freedoms of the data subject

fogler rubinoff

What's the US Doing?

- Taken from OPC's Consent Paper May 2016
- Current – Patchwork of federal and state laws
  - Reflect harm-based approach to privacy; many are sector specific (e.g., health information)
  - Fair Information Practice Principles are the basis of privacy protections and "notice and choice" is a core element
  - US Federal Trade Commission (**FTC**) promotes consumer privacy under the unfair and deceptive practices provisions of the FTC Act

fogler rubinoff

What's the US Doing?

- Proposed – Consumer Privacy Bill of Rights – Feb 2015
  - Consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which consumers provided the data
  - Has been criticized as having weak enforcement provisions
  - If a company processes personal data that is not reasonable in light of context, it must conduct a privacy risk analysis and take reasonable steps to mitigate any privacy risks identified as a result

fogler rubinoff

What's Canada Doing?

OPC's Discussion Paper on Possibly Enhancing the Consent Model under PIPEDA – May 2016

- Invited submissions (due end of July) to answer specific questions
- Describes challenges to meaningful consent under privacy law
  - New technologies and business models (like BD and IoT)
  - Human behaviour
- Surveys how consent is treated in the EU and US
- Discusses possible solutions
  - Enhancing consent
  - Alternatives to consent
  - Improved governance/stewardship
  - Enhanced enforcement

fogler rubinoff

What's Canada Doing?

OPC's Consent Paper – Human Behaviour

- PIPEDA's knowledge and consent requirements make individuals responsible to inform themselves of an organization's privacy practices ... But this is easier said than done
- Not only because of the complexities of the digital ecosystem (e.g., the IofT and BD) but also the paradoxes of human behaviour and the reality of an individual having limited time, interest and energy to fully engage with an organization's privacy policies
- There is lots of evidence that human behaviour undermines the efficacy of the consent model under PIPEDA
- Many studies have found that individuals who say they care about their privacy rights at the same time disclose vast amounts of personal information online

fogler rubinoff

What's Canada Doing?

OPC's Consent Paper – Human Behaviour

- The explanations for this include:
  - Individuals often find it tough to quantify privacy risks when compared to specific rewards of disclosing their PI online
  - Individuals may not appreciate the privacy implications of what they are disclosing, especially over time as small incremental disclosures paint a bigger picture
  - Individuals are easily fooled by the illusion of privacy – e.g., via prominent privacy policies and privacy trust marks
  - While individuals do not want to lose control over their PI, many believe this loss of control has already happened – and so are inclined to give out their PI as a trade-off for benefits they receive

fogler rubinoff

What's Canada Doing?

OPC's Consent Paper – Possible Solutions

- Enhancing consent by:
  - Greater transparency in privacy policies and notices
  - Managing privacy preferences across services
  - Technology-specific safeguards
  - Privacy as a default setting – privacy by design (PbD)

fogler rubinoff

What's Canada Doing?

OPC's Consent Paper – Possible Solutions

- Alternatives to consent such as:
  - De-identification
  - No-Go Zones (both "true" and "proceed with caution")
  - Legitimate business interests

fogler rubinoff

What's Canada Doing?

OPC's Consent Paper – Possible Solutions

- Improved governance and accountability through:
  - Codes of Practice
  - Privacy Trust marks
  - Ethical Assessments

fogler rubinoff

What's Canada Doing?

OPC's Consent Paper – Possible Solutions

- Stronger enforcement:
  - Proactive enforcement activity
  - Perhaps giving the OPC order-making powers (and the ability to levy fines)

fogler rubinoff

CMA's Perspective

Submission of Canadian Marketing Association (CMA) to OPC's Consent Paper Consultation – August 2016

- CMA submits that the best approach to strengthening privacy protection of individuals (given the challenges of today's digital advertising ecosystem) is a combination of:
  - strengthening the accountability framework and
  - expanding the use of implied consent

fogler rubinoff

CMA's Perspective

- Consent should evolve by shifting the focus from a rigid interpretation of "notice and consent" to an enhanced ombudsperson and accountability framework that would allow organizations more flexibility in the way they collect, use and disclose PI

fogler rubinoff

CMA's Perspective

- PIPEDA's current framework could be enhanced by
  - expanding the recognition and use of implied consent
  - the development by stakeholders of more relevant and targeted codes of practice
  - greater use of de-identification
  - allowing the processing of PI without consent for legitimate interests
  - making the definition of publicly available information under PIPEDA technology neutral

fogler rubinoff

CMA's Perspective

- CMA takes some positions that seem to be at odds with those expressed in the OPC's Consent Paper – for example, that:
  - PIPEDA already recognizes that organizations may process PI for legitimate interests without consent (in 4.3.3 of Schedule 1)

    [But CMA says it would "nonetheless help to explicitly permit the processing of PI without individual consent for legitimate purposes and to clarify under what circumstances"]

fogler rubinoff

CMA's Perspective

- CMA also says the risks of re-identification are overblown ("very theoretical, even hypothetical, speculative and abstract")
- What's needed, in the CMA's view, are practical rules around de-identification and that assessments about the risk of re-identification should focus on the actual risk of re-identification and the technical and contractual measures an organization has put in place to address those risks
- CMA suggests there is a useful model in the UK Information Commissioner's Office *Anonymization: Managing Data Protection Risk Code of Practice*

Thank You

Bill Hearn, Partner
Fogler, Rubinoff LLP

77 King Street West, Suite 3000
TD Centre North Tower
Toronto, ON M5K 1G8

416.941.8805
bhearn@foglers.com