


Fall 10-18-2012

Who's in Charge Here? Information Privacy in a Social Networking World

Lisa Di Valentino

The University of Western Ontario, ldivalen@uwo.ca

Follow this and additional works at: <https://ir.lib.uwo.ca/fimpspres>

 Part of the [Communications Law Commons](#), [Communication Technology and New Media Commons](#), [Computer Law Commons](#), [Conflict of Laws Commons](#), [Internet Law Commons](#), and the [Library and Information Science Commons](#)

Citation of this paper:

Di Valentino, Lisa, "Who's in Charge Here? Information Privacy in a Social Networking World" (2012). *FIMS Presentations*. 15.
<https://ir.lib.uwo.ca/fimpspres/15>

WHO'S IN CHARGE HERE?

Information
privacy in a
social
networking
world

Lisa Di Valentino
October 18, 2012



OUTLINE

1. Social networking services usage and business models.
2. Overview of Canadian law relating to personal information privacy protection.
3. Overview of U.S. law relating to personal information privacy protection.
4. Privacy policies and terms of service.
5. Conflict of laws: Which laws apply?
6. Current proposals.
7. Discussion.

SOCIAL NETWORKING SERVICES

Who's in charge here?

SNS USAGE



Members as of August 2012

World: 175 million

Canada: 6 million

Members as of March 2012

World: 500 million

Canada: 200,000

source:

<http://techcrunch.com/2012/07/30/an-alyt-twitter-passed-500m-users-in-june-2012-140m-of-them-in-us-jakarta-biggest-tweeting-city/>

source: <http://press.linkedin.com/about>

SNS USAGE



Members as of October 2012

World: **1 billion**

Canada: **18 million**

(68.7% of Canadian Internet users)

source: <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>

IMPLICATIONS OF SNS POPULARITY

- personal information is no longer incidental to a consumer transaction
- it has become the “currency” that users provide to pay for the service
- SNSs leverage the information to create value for the service
- as more individuals participate, the SNS becomes more valuable
- users are “co-developers” through participation

SNS BUSINESS MODELS

- three main approaches SNSs take to generating revenue
- 1) Subscriptions
 - users pay a fee for access to certain services
 - LinkedIn uses a “freemium” model – users can access the basic functions of the site for no charge, but can also pay a monthly fee for services such as direct messaging
- 2) Transactions
 - SNS provides environment for a monetary transaction in return for a fee or percentage of the price
 - Facebook applications where users can make purchases within the game

SNS BUSINESS MODELS

- 3) Advertising
 - Twitter “promoted tweets” places the name of a sponsoring organization at the top of the trending topics list
 - Facebook also allows third parties to display advertisements on user pages
 - information supplied by users may be used to personalize or target advertisements, either in aggregate or individually
- an SNS may use any one or a combination of approaches; e.g. LinkedIn uses both subscription and advertising
- Facebook and Twitter rely on advertising

REGULATIONS

Who's in charge here?

FAIR INFORMATION PRACTICE PRINCIPLES

- developed by Organisation for Economic Cooperation and Development (OECD) in 1980
- not law but rather a guide for best practices
- basis for data privacy legislation in many jurisdictions, such as Canada, the U.S., and the EU
- eight core principles of privacy protection for personal information

FAIR INFORMATION PRACTICE PRINCIPLES

Collection Limitation

Data Quality

Purpose Specification

Use Limitation

Security Safeguards

Openness

Individual Participation

Accountability

LEGISLATION: CANADA

- Office of the Privacy Commissioner is the federal body responsible for safeguarding Canadians' data privacy
- acts as ombudsperson, investigating complaints and making recommendations
- two federal laws protecting Canadians' personal information
- *Privacy Act*, RSC 1985, c P-21
 - applicable to (federal) public sector use of personal information
- *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA)
 - applicable to private sector use of personal information

PIPEDA

- enacted in 2000 and fully implemented in 2004
- applies to all organizations in Canada that collect, use, or disclose personal information in the course of commercial activities (s 4(1))
 - except in B.C., Alberta, and Quebec, which have substantially similar provincial privacy laws
- limits how organizations can collect personal information and what they can do with it

PIPEDA

- *personal information* is defined as “information about an identifiable individual, but does not include the name, title, business address, or telephone number of an employee of an organization” (s 2(1))
- organizations may collect, use, or disclose personal information only for purposes a reasonable person would consider appropriate in the circumstances (s 5(3))
- personal information may only be collected with individual’s knowledge and consent, except in special circumstances (cl 4.3.1)

PIPEDA

- collection of personal information shall be limited to that which is necessary for the purposes identified by the organization (cl 4.4)
- organizations shall not collect personal information indiscriminately (cl 4.4.1)
- personal information shall not be used or disclosed for purposes other than those for which it was collected, except with consent or as required by law (cl 4.5)

PIPEDA

- consent must be meaningful and purposes must be stated in such a way that the individual can reasonably understand how the information will be used or disclosed (cl 4.3.2)
- reasonable expectations of individual are relevant to obtaining consent (cl 4.3.5)
- knowledge or consent is not required when information is publicly available and is specified by the regulations (s 7(1)(d))
 - *Regulations Specifying Publicly Available Information, SOR/2001-7*
 - s 1(e) personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information

PIPEDA: REMEDIES

- Privacy Commissioner may investigate complaints and issue reports and recommendations, but cannot directly intervene
- any remedies must be pursued through the federal court by the individual or Commissioner
- does not allow for statutory damages; a complainant must prove that he in fact suffered damages
 - pecuniary injury must have been a direct result of the breach of privacy rights

FACEBOOK FINDINGS 2009

- in 2009 CIPPIC filed a complaint against Facebook with the Office of the Privacy Commissioner
- Office's report found that certain of the allegations were well-founded (in other words, Facebook had contravened PIPEDA in certain ways):
 - Facebook did not adequately explain the purpose for and use of certain required information (date of birth)
 - Facebook did not make a reasonable effort to provide sufficient notification to users before using their information for advertising purposes (Social Ads)
- Facebook made changes to its privacy policy and no further action was taken by the complainants or the OPC

COMMON LAW

- *Jones v Tsiges*, 2012 ONCA 32
- Sharpe J formulated a tort of invasion of privacy based on "intrusion upon seclusion"
- narrowly defined as an intentional intrusion upon someone else's private affairs that would be highly offensive to a reasonable person

LEGISLATION: UNITED STATES

- the United States does not have a similar omnibus federal information privacy law applicable to the private sector
- instead, these laws have developed in a piecemeal fashion, as part of other pieces of federal legislation
 - *Telecommunications Act* (protection of customer network data)
 - HIPAA Privacy Rules (medical records)
 - *Right to Financial Privacy Act* (financial information)
 - *Video Privacy Protection Act* (video rental records)
 - *Stored Communications Act* (addresses unlawful access to stored communications)
- but generally left up to the private sector

LEGISLATION: CALIFORNIA

- states may also have their own information privacy laws
- of all the states, California has the strongest information privacy laws (although relatively weak compared to Canada and the EU)
- Facebook, Twitter, and LinkedIn are headquartered in California
- data privacy is addressed in bits and pieces throughout the state's penal and civil codes

LEGISLATION: CALIFORNIA

- Internet Privacy Requirements of the Business and Professions Code requires that operators of commercial websites that collect personally identifiable information have a conspicuously posted privacy policy
- policy must inform users of the categories of information that are collected, and the categories of third parties with whom the information may be shared
- but there is no requirement to disclose how the information may be used
- violators may face court action by the Attorney General; penalties include injunctions and fines
- but... this law only protects residents of California

COMMON LAW

- California recognizes the tort of invasion of the right of privacy
- appropriation of another's name or likeness: defendant has used the plaintiff's name or likeness to advertise its commercial endeavour
- public disclosure of private facts: the facts in question are not of legitimate public concern and are of a kind that would be objectionable to the reasonable person

FEDERAL TRADE COMMISSION

- FTC is responsible for investigating alleged unfair practices, including those related to personal information
- developed guidelines for organizations that collect and use personal information (based on Fair Information Practice Principles)
 - recommendations only and do not have the force of law
- may hold hearings and make orders against organizations that have been found to engage in deceptive or unfair practices

FEDERAL TRADE COMMISSION

- March 2011, FTC found that Google engaged in unfair or deceptive acts
- Google's privacy policy had stated that user information would not be used for other purposes without user's consent
- when the company launched Google Buzz (social networking service), users found that their contact lists were made public
- Google opted to settle rather than face a hearing and a possible fine of \$10,000 per violation

FEDERAL TRADE COMMISSION

- November 2011, FTC alleged that Facebook engaged in deceptive or unfair business practices
- claimed that it changed its privacy policy retroactively, and without the informed consent of users, making users' friends lists public
- Facebook agreed to a consent order prohibiting it from misrepresenting the privacy protection of personal information

PRIVACY POLICIES & TERMS OF SERVICE

Who's in charge here?

PRIVACY POLICIES

- the most popular SNSs have privacy policies that typically outline what information is collected from users, how the sites use the information, and with whom it is shared
- federal U.S. laws against unfair or deceptive practices oblige sites to act in accordance with stated policies
- SNS users rarely read privacy policies, citing length and difficulty of comprehension
- a 2011 poll of Canadian Internet users found that only 21% “always” or “often” read web sites’ privacy policies

TERMS OF SERVICE

- SNSs provide users with services subject to terms of service agreements (TOS) which outline the respective obligations of the site and the users, incorporating privacy policies by reference
- inevitably include “choice of forum” and “choice of law” clauses by which the user agrees to settle disputes according to the law of a certain jurisdiction
- Facebook’s and LinkedIn’s clauses indicate that disputes will be heard in the courts of Santa Clara County, and governed by the laws of California
- Twitter’s TOS provides that disputes will be heard in San Francisco County

WHOSE LAWS APPLY?

Who's in charge here?

CONFLICT OF LAWS

- PIPEDA does not explicitly address its application outside of Canada
- the plain text of the law does not limit its application to Canadian organizations, but it doesn't specifically provide for extraterritorial effect
- *Lawson v Accusearch Inc*, 2007 FC 125
 - Federal Court held that the OPC had the jurisdiction to investigate the actions of Wyoming-based Accusearch because it collected and communicated personal information in Canada
 - [however, this ratio cannot necessarily be applied to court actions]

CONFLICT OF LAWS

- as a preliminary matter, the express choice of law clause must be taken into consideration
- generally, Canadian courts (with the exception of those in Quebec) treat choice of law and forum clauses with a certain amount of deference
- the party challenging the clause must demonstrate a strong reason that it should not be given effect
- must show that it was not made in good faith, is not legal, or is contrary to public policy

CONFLICT OF LAWS: WHAT TO DO?

- assuming that the choice of law and forum clauses are given effect, a Canadian (non-Quebecker) would be obliged to pursue an action in California courts
- some of the shortcomings with this scenario include:
 - Internet Privacy Requirements do not provide the same substantive protection as PIPEDA, and only apply to California residents
 - state's laws against unfair business practices do not provide for a civil suit by a wronged individual, only an action by the Attorney General
 - tort action based on public disclosure of private facts would require that the information revealed is objectionable to the reasonable person
 - tort of appropriation of name or likeness requires that there is some external value associated with the plaintiff's identity

CONFLICT OF LAWS: WHAT TO DO?

- one option would be to request that the Federal Trade Commission investigate the impugned practices on the basis of unfairness or deception
- *FTC Act* provides that restitution may be paid to domestic or foreign victims
- or file a complaint with the OPC, to whom choice of law and forum clauses do not apply
- should an SNS choose to not implement the OPC's recommendations, the OPC has the option to initiate a heading in Canadian federal court

CURRENT PROPOSALS

Who's in charge here?

PROPOSALS

- PIPEDA up for 5 year review (last year)
 - Jennifer Stoddart wants better enforcement mechanisms and stronger financial penalties for business that violate the statute
- bills introduced to U.S. Senate and Congress
 - proposals for comprehensive information privacy law
 - White House's plans for a "Do Not Track" law
- international treaties
 - no data privacy treaties as yet, but several guidelines, memoranda, recommendations, and resolutions
 - 2008 Rome Memorandum (privacy in social networking)

DISCUSSION

Who's in charge here?

DISCUSSION

Do you think that personal information protection should be left up to the individual social networking service user (as through contracts or simply not revealing personal information online?) Or is it necessary for the government to step in?

Is such information even “private” once it’s posted on a social networking site?

Has the nature of privacy itself changed in the social networking era?