CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Philanthropy Forum 2016
Community Foundation of Greater Peterborough
November 15, 2016

LEGAL ISSUES IN SOCIAL MEDIA FOR CHARITIES

By Terrance S. Carter, B.A., LL.B., TEP, Trade-mark Agent
tcarter@carters.ca

OVERVIEW

- Introduction
- Why This Topic Matters
- Benefits of Using Social Media
- Pitfalls of Using Social Media
- Privacy Issues with Using Social Media
- CRA Regulatory Issues with Using Social Media
- Intellectual Property Issues with Using Social Media
- Other Legal Areas of Concern
- Social Media Risk Management
- Conclusion

A. INTRODUCTION

- With the use of social media continuing to rise, the purpose of this presentation is to discuss the various legal aspects of social media

B. WHY THIS TOPIC MATTERS

- What you post on social media pages can have various implications, which may include:
  - Privacy law suits or complaints to the relevant Privacy Commissioner
  - An organization could be held liable in other ways (e.g., libel, copyright infringement, etc.)
  - Disciplinary measures, which might include termination of employment or loss of charitable status by the CRA

C. WHAT IS SOCIAL MEDIA?

- Websites and applications that enable users to create online communities where they can share content or network with others
- Social media sites are based on user participation and user-generated content
- Social networking sites provide users with the ability to upload profiles, post comments, links, photos, videos, join “networks”, and add “friends”
- Social media equals “private broadcasting”

- Examples of Social Media:
  - LinkedIn
  - Facebook
  - Twitter
  - Instagram
  - Pinterest
  - Snapchat
  - YouTube
  - Reddit
  - Google+
  - Blogs, websites, etc.

D. BENEFITS OF USING SOCIAL MEDIA

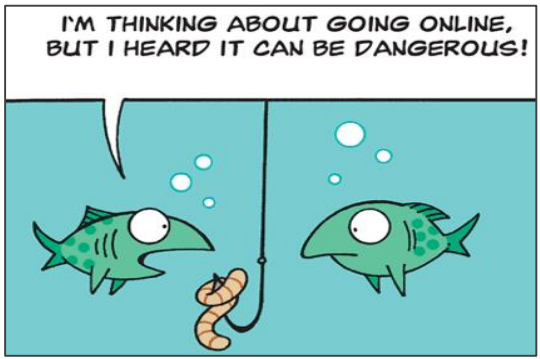
- It's very inexpensive
- It offers a quick way to target new markets
- It helps expand your audience and reach
- It helps your supporters to spread the word about you
- It can assist with employment and volunteer recruitment
- It allows you to receive instant feedback

- It helps to increase website traffic
- It allows sharing of content in a timely manner
- It strengthens relationships with donors, volunteers, and partners on a more personal level
- It helps to increase brand awareness with little to no budget

E. PITFALLS OF USING SOCIAL MEDIA

- Given all of these benefits with using social media, it might be hard to envision any negative consequences with using social media
- Negative consequences though, could occur in an individual's personal capacity as an employee of an organization, and for the organization itself

- As such, prior to launching a social media campaign, it is important to consider the pitfalls of doing so, including:
  - Privacy Issues
  - CRA Regulatory Issues
  - Intellectual Property Issues
  - Other Issues of Concern



F. PRIVACY ISSUES WITH USING SOCIAL MEDIA

- The privacy issues that arise with the use of social media are the focus of our discussion today because the evolution of information sharing online has called into question how social media impacts individuals' privacy

- Social media has spurred a change in how individuals and organizations view and protect personal information
- We share a lot of personal information online (e.g., birthdays, relationship status, and much more)
- As a result, Canadian courts are continually carving out new privacy laws to keep up with the changing landscape

- The information posted on social media sites may breach applicable privacy laws
- There is no express exemption to privacy laws for charities and not-for-profits
- There are privacy laws in Canada (discussed below) that prevent individuals from using other individuals' "personal information" without their knowledge and consent
- Posted content is often considered personal information and may be subject to privacy laws

1. What is Personal Information?

- “Personal information” is defined in privacy legislation as “any information about an identifiable individual”
- It does not include anonymous or non-personal information (i.e., information that cannot be associated with a specific individual)
- Examples of personal information include an individual's name, address, social insurance number, and photos or videos of individuals

2. Key Canadian Privacy Laws that May Apply to Social Media Use

- Federal private-sector legislation (PIPEDA) and “substantially similar” provincial legislation
- Ontario public-sector privacy legislation
- Privacy torts

3. PIPEDA and "Substantially Similar" Provincial Legislation

- The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is the main private-sector legislation for protecting privacy in all provinces that have *not* enacted "substantially similar" legislation
- An organization may be exempt from PIPEDA if the province has enacted privacy legislation that is declared "substantially similar" to PIPEDA
- In that case, the substantially similar provincial legislation would then apply instead of PIPEDA

- Alberta, British Columbia, and Quebec have passed substantially similar legislation
- Ontario, New Brunswick, and Newfoundland have passed substantially similar legislation with respect to personal *health* information
- In Ontario, the substantially similar private-sector legislation is the *Personal Health Information Protection Act* (PHIPA)
- Organizations dealing with personal health information need to consider this legislation
- In Ontario, the public-sector FIPPA governs "institutions" (e.g., hospitals, universities) use of non-health personal information (see below)

- All privacy legislation establishes ground rules for the management of personal information and aims to strike a balance between the right to privacy and the need for organizations to collect, use, and disclose personal information
- The same principles found in PIPEDA are also found in the substantially similar provincial legislation

4. Key Principles from Privacy Legislation

- An organization is responsible for personal information under its control
- Policies and practices regarding the management of personal information must be implemented
- An individual must be designated to oversee compliance with applicable legislation (“Privacy Officer”)
- Contracts which provide for protection of personal information should be in place with any third party, e.g., data processors, partners, affiliates

- These contracts should consider:
  - The “ownership” of personal information of donors, beneficiaries, etc.
    - Ensure this is clear to avoid future issues
  - The storage of personal information
    - Privacy law does not prohibit the storage of data outside of Canada, but there are administrative hurdles which must be met
    - Importantly, CRA’s position is that books and records must be kept “at an address in Canada recorded with the Minister”
    - Servers outside of Canada are problematic

- Purposes for using personal information must be identified and documented at or before the time the information is collected
- Purposes must be those that “a reasonable person would consider appropriate in the circumstances” considering the sensitivity of the information
- The collection of personal information should be limited to that which is necessary for the purposes identified
- Personal information must be protected by appropriate safeguards

- Minor's personal information (including photos) require express consent (but can be challenged)
- Subject to limited exemptions, the knowledge and consent (implied or express) of the individual are required for the collection, use, or disclosure of personal information
  - E.g., personal information collected from a donor cannot be transferred to another charity without express consent
- When personal information that has been collected is used for a new purpose, the consent of the individual is required before information can be used for that new purpose

5. Ontario Public-Sector Legislation

- *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to the provincial government and many "institutions", e.g., hospitals, universities
- While FIPPA governs the use of non-health personal information held by hospitals, as discussed above, personal *health* information held by hospitals is governed by PHIPA (and not FIPPA)

- Although hospital foundations are not directly subject to FIPPA, it has an impact on foundations and hospitals' ability to share information with foundations for fundraising
- Foundations may collect personal information independently from the hospital (i.e., donor personal information that is provided directly to the foundation rather than to the hospital)
- As such, the collection of such personal information will not be subject to FIPPA (though it may be subject to other privacy legislation)

- FIPPA has two main purposes. It establishes:
  - **a privacy protection regime** for personal information held by "institutions" - applies to the sharing of information by hospitals with foundations, e.g., for fundraising
  - **a freedom of information regime** requiring institutions to respond to requests for access to records – may include any hospital records about a foundation, and any foundation records held by a hospital (subject to certain exclusions, e.g., records relating to the operations of a hospital foundation and to charitable donations made to a hospital)

- In the context of fundraising, hospitals and their foundations must be compliant with FIPPA
- FIPPA provides that a hospital may use personal information for fundraising if the use is "reasonably necessary" for its fundraising
- FIPPA outlines requirements for the hospital in using information for fundraising, including:
  - certain notice requirements
  - that hospitals have fundraising agreements with any persons to whom personal information will be disclosed for fundraising (e.g., hospital foundation)

- Hospital foundations should work with associated hospitals and legal counsel to develop policies for the sharing of foundation information generally, as well as the exchange of records between foundations and hospitals
- This can help to clarify and standardize information-sharing practices and minimize the risk that potentially sensitive foundation records will be unnecessarily or unintentionally disclosed
- Hospital foundations should also acquaint themselves with their hospital's FIPPA-related policies and procedures

- Several privacy acts may apply to one organization
- E.g., in Ontario, hospitals are governed by:
  - PHIPA with respect to personal health information
  - FIPPA with respect to non-health personal information
  - PIPEDA with respect to activities that are not core to its operations, e.g., personal information collected by a hospital while operating a parking garage

6. Privacy Torts

- There are also "judge-made" privacy torts (i.e., a civil personal wrong) in Ontario
- In *Jones v. Tsige*, 2012, the Ontario Court of Appeal recognized the tort of "intrusion upon seclusion" which is essentially, breach of privacy
- The Court stated that the tort occurs when:
  - "The conduct complained of is intentional or reckless, the person's private affairs or concerns were unlawfully invaded, and a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish"

- In *Doe 464533 v. N.D.*, 2016, the Ontario Superior Court of Justice recognized the tort "public disclosure of private facts"
- The Court stated that the tort occurs when:
  - "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized, or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public"

G. CRA REGULATORY ISSUES WITH USING SOCIAL MEDIA

- Does your online presence accord with your stated charitable objects?
  - This is important for both organizations seeking charitable status and those that already have charitable status
  - CRA will review your online content, including the materials to which your organization links, to see if it accords with the information provided in your application

- Relevant considerations:
  - Does website content indicate programs outside of your stated purposes?
  - Does your website link - and therefore by implication agree and endorse - problematic materials?
  - Does your website content indicate prohibited activities?

- Does your online presence include materials that could lead to revocation?
  - Be cautious of what is posted on social media sites about your organization
  - CRA auditors will review website content for information and data that will support cause for revocation
  - This can include links to other organizations, as well as reviewing internet search history for the organization's computers

H. INTELLECTUAL PROPERTY ISSUES WITH USING SOCIAL MEDIA

- Register and enforce IP
  - An organization's brand is one of its most important assets - it distinguishes the organization from other organizations
  - With social media, branding reaches a large audience around the world in an instant
  - Failing to register trademarks prior to using them online can lead to third parties poaching and registering marks prior to the owner

- Trademarks can be lost if they are not properly protected
- An organization needs to be pro-active in protecting its trademarks or it may risk losing its trademark rights by default
- Registration of a corporate name or business name does not by itself give trademark protection
- Once registered, ensure marks are properly used on social media
  - E.g., train staff on proper usage, proper markings, and consistent usage

- Ensure IP of others is not infringed
  - Social media can expose your organization to liability for infringing the intellectual property rights of others
  - Monitor social media sites for postings by employees and third parties that may infringe trademarks or copyrights of others
  - Review posted content and consider who is the owner of the work
    - If the organization does not own the work, any reproduction of that work on social media can constitute copyright infringement

- Generally, the *author* of the work is the *owner*, unless an exception exists, such as:
  - Work made in the course of employment vests in the employer, unless there is an agreement to the contrary
  - Author must be human - corporations cannot be an author
- The above applies only to “work made in the course of employment” by employees
  - Independent contractors and volunteers are not usually considered employees
- All employment contracts should be reviewed by legal counsel

I. OTHER LEGAL AREAS OF CONCERN

- Employees' use of social media
  - Employees may reveal confidential information intentionally or inadvertently
  - Employees may use trademarks incorrectly, leading to dilution and weakening of an organization's brand
  - Employees may infringe the IP of others

- Electronic discovery and evidence
  - Information can be used as evidence in litigation
- Libel, cyber-stalking, cyber-bullying
  - The content could be defamatory or lead to cyber-stalking or cyber-bullying (criminal offences)
- Data breaches
  - Third parties “hacking” into the social media page and inappropriately using it to tarnish reputation
- Large audience
  - Although this is a benefit, it is also an issue - once something is posted, it reaches a world-wide audience immediately, and is open to individual criticism and interpretation - once posted, it’s impossible to control or get back

J. SOCIAL MEDIA RISK MANAGEMENT

- In order to help understand and minimize the legal risks associated with using social media, some of the policies and practices that an organization should implement, with the assistance of legal counsel, include the following:

1. Implementing a social media policy
2. Implementing a privacy policy
3. Updating employment contracts and policies
4. Ensuring all IP is protected

1. Implementing a Social Media Policy

- Keep in mind that there is no “one size fits all” policy; it will need to be adapted to fit the needs of the particular organization and its employees
- Organizations should carefully consider what it wishes to include in the policy and ensure that it is consistently implemented
- For example, does the social media policy only reflect the use of the employer’s official social media pages, or the use of employees’ personal social media pages as well?

- Amongst other things, the Social Media Policy may outline the following:
  - A very broad definition of social media which captures the use of email and internet surfing
  - No one may violate the privacy of another person (e.g., disclosure of salary)
  - Proprietary information belonging to the organization may not be disclosed
  - Restricted behaviours, such as posting material deemed inappropriate or which could discredit or cause embarrassment to the organization

- Who is allowed to post “official” social media communications on behalf of the organization
- Use of the organization’s name or other trademarks or copyright on social media pages require consent
- Make reference to other relevant policies such as employment policy, privacy policy, etc.

- Encouraging the use of a disclaimer such as,*"The views expressed on this website are mine alone and do not necessarily reflect the views of [name of particular Organization]"*
- Include prohibitions on speaking on behalf of the organization

- Outline acceptable practices regarding using the organization's IT systems for accessing social media
- For example, the policy may provide that:
  - An organization may monitor use of its IT systems and as such, the organization's IT systems should not be used for personal use
  - If the IT systems are used for personal use, then the individual acknowledges that they have no expectation of privacy in connection with that use

- Use of personal IT systems (such as personal cell phones) for accessing social media during work hours, should be limited to pressing circumstances, such as family emergencies
- Use of personal IT systems is not subject to monitoring, so it is clearly the preferred means of personal communication for employees

2. Public Privacy Policy

- Privacy laws in Canada require organizations to be open about their personal information handling practices
- Organizations should implement a “public facing” privacy policy which is posted on the website
- In the event of an investigation, the privacy policy will help to demonstrate to the relevant Privacy Commissioner that the organization is an accountable organization with up-to-date privacy management programs in place

- Amongst other things, the public privacy policy should outline the following:
  - How personal information will be used, collected, and disclosed
  - How personal information is safeguarded
  - The process for making and handling complaints
  - The process for dealing with data breaches
  - Identify the Privacy Officer and include contact information

3. Updating Employment Contracts

- Employment contracts should be reviewed to:
  - Ensure they clearly state that the organization is the owner of all work and that moral rights are waived
  - Ensure that similar contracts are in place for volunteers, website designers, independent contractors, etc., otherwise the copyright vests in these entities by default
  - Ensure reference is made to the various employment policies, such as the social media policy

4. Ensuring all IP is Protected

- Protect your IP before posting it online
  - Avoid a costly branding blunder by completing the necessary due diligence ahead of time
  - Conduct trademark clearance searches to ensure marks are not encroaching on others' marks before using them on social media
  - Register all trademarks, copyrights, and domain names to avoid poaching by third parties

5. Always Review Social Media Content

- Consider CRA issues
- Consider other legal issues
- Immediately take down inappropriate content

K. Conclusion

- Although social media can have many benefits, it is important to remember that discretion and common sense should be used when posting on social media pages
- One way to manage the risk associated with social media is to ensure that the various policies discussed today are implemented and reviewed on an ongoing basis

CARTERS

BARRISTERS
SOLICITORS
TRADEMARK AGENTS

Disclaimer

This handout is provided as an information service by Carters Professional Corporation. It is current only as of the date of the handout and does not reflect subsequent changes in the law. This handout is distributed with the understanding that it does not constitute legal advice or establish a solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can be relied upon for legal decision-making. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.