Office of the
Privacy Commissioner
of Canada

Online Reputation

What are they saying about me?

Discussion Paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada

Table of Contents

Abstract

This discussion paper looks at the issue of online reputation from a privacy perspective, and sets out the challenges faced by individuals whose online information has a negative impact on their reputation. By discussing the experiences of the Office of the Privacy Commissioner of Canada (OPC) to date, we hope to advance the discussion on how best to provide individuals with recourse when their online reputation is negatively affected by information they themselves or others have posted about them. We will seek stakeholder feedback, with the ultimate aim of putting forth a position on solutions.

Introduction

In 2015, the OPC chose Reputation and Privacy as one of the Office's privacy priorities for the next five years. The Office is focusing its attention on the reputational risks stemming from the vast amount of personal information posted online and on existing and potential mechanisms for managing these risks. During the OPC's Priority Setting Exercise, we heard from stakeholders and the Canadian public that while they recognize the personal and professional benefits of participating in the online world, they are increasingly concerned about their online reputation.

On one hand, individuals want an online presence and believe that being selective in what they post will help shape their online reputation. On the other hand, individuals have little control over what others post about them and how their personal information might be interpreted by individuals and organizations.

Shakespeare wrote: "Reputation is an idle and most false imposition; oft got without merit, and lost without deserving."[1] Never has this been more true than in the digital environment, where information "is not simply posted; it is manipulated, mined and interpreted."[2] In addition, everything posted online is potentially viewable and shareable by millions, and it could surface months or years after posting, in a variety of contexts, intended or not.

Since the advent of social media, much has been written about online reputation and how it can affect people's lives, both online and off. Internet technologies have caused a paradigm shift in the way reputations are formed, and society is grappling with the impact on social relationships and professional opportunities. A more robust discussion is needed about the recourse available to people who object to the personal information that is posted about them online.

With this paper, our aim is to start a discussion about potential ways to address issues associated with the permanency of personal information online and the effect on reputation. We are calling on individuals, organizations, academics, advocacy groups, information technologists, educators and other interested parties to generate ideas for new and innovative ways to protect and enhance reputational privacy. To guide the discussion, we have set out the Office's experiences and thoughts about the limitations and challenges associated with people's ability to control their online privacy. We are inviting submissions from interested parties on potential solutions to some of the questions outlined at the end of the paper, with a view to developing an OPC position on how reputational issues may best be addressed.

Reputation and Privacy

The Oxford Online Dictionary defines reputation as "the beliefs or opinions that are generally held about someone or something" and "a widespread belief that someone or something has a particular characteristic."[3] Such beliefs and opinions are based on information that is available about individuals, and on the manner in which this information is interpreted and assessed by others. Reputation is a form of judgment of an individual's character, appearance, professional skills – any attribute that is subject to opinion. Individuals' ability to affect others' judgments and thus manage their reputation depends on their ability to control the availability of their personal information to others and the context in which it is accessed and used.

The type and amount of information people choose to disclose about themselves tends to depend on the circumstances at hand. Over 50 years ago, sociologist Erving Goffman[4] used the metaphor of a theatrical performance to describe how individuals present themselves, and how much information they reveal about themselves, on the public "stage" versus in a more intimate "backstage" space. In public, social exchanges are guided by individuals' understanding of the standards of behaviour that pertain to their social group. In a more private setting, individuals feel more at ease, and more free to express themselves rather than follow a "script."

Offline, people have more opportunities to influence how others perceive them in a variety of ways, such as through their behaviour, appearance, accomplishments, and communication skills. Information is also slower to spread in the physical world. The development of reputations online is more complicated because, in the digital environment, judgments are generally formed on information people read about others, or images they see, often without the benefit of personal contact and not necessarily in the same context in which it was intended. Moreover, information, once posted online, gains characteristics that affect reputation.

Some features of online reputation

Social media scholar and Microsoft Principal Researcher danah boyd characterized information posted on online social networking sites as having four distinct features,[5] and her ideas readily translate to the digital realm in general. First, online information is persistent, in that it is in recorded form, and deleting it once it has been uploaded is challenging, if not impossible. Online information can be replicated. It is also potentially visible to a vast and unintended audience. Finally, it can be accessed through a search function.

Another way of conceptualizing how information is transformed online and how this affects reputation is the "house of mirrors" analogy outlined by Johnson, Regan and Wayland in their paper [6] about the impact of the Internet on the accessibility of public records. The authors make the case that the process of giving the public access to public records needs to be reconsidered, with privacy at top of mind, given that the Internet distorts information just like a house of mirrors distorts images. Of particular relevance to the discussion on privacy and reputation is the following:

> *A house of mirrors is a complex of imagery, with bouncing, highlighting, and shading of images that produce a surprising experience. An individual sees an image of him or herself out of whack with their ordinary sense of self*.

"Bouncing" refers to information that has been posted for one purpose and subsequently is used for another. An example of bouncing would be the act of scraping a photo from a social media site and selling it to an advertising agency, as happened to an American family whose personal photo ended up on a billboard advertising a Czech grocery store.[7] In another, particularly egregious, example, a Swiss bio-medical firm used a photo of a Canadian child to advertise genetic tests for Down's syndrome. The photo was taken without permission from her mother's blog.[8]

"Highlighting and shading" is the notion that information can gain or lose value depending on the context. As a result, information can play a distorted role in shaping an individual's reputation. For example, information that appears at or near the top in search results is "highlighted" no matter how trivial it might be, while potentially pertinent information, if it appears low in search results, would be "shaded." Research[9] has shown that those scanning search results tend to focus their attention at the top of the page. When it comes to clicking on links, the study results[10] are more dramatic, with the vast majority of people only selecting links on the first page of search results. This type of pre-selection of information can have a negative effect.

Take for example the emergence of the subculture of humiliation[11] where people are belittled for "fun" in popular media, and incidents of online shaming or cruelty can garner millions of views. Since search engine algorithms typically surface the most popular information regardless of its content, viral content can thus be inadvertently

promoted over, and often at the expense of, more pertinent and representative information about the individual. In an extreme example[12] of the harm that can occur, the parents of a California accident victim tried for several years to stop photos of her disfigured body from being circulated online. The accident scene photos were leaked by law enforcement employees and appeared on thousands of websites, along with cruel comments. While the family was able to obtain a settlement from the law enforcement authority, the images continue to be easily found through search engines.

Social media by its very definition is based on individual participation and sharing of content. Users are encouraged to upload information about themselves and others as they navigate the digital world. From comments sections and photo-sharing sites to blogs and social networks, there are endless opportunities to provide personal information. Indeed, some features specifically ask users to divulge information about people they know, for example, uploading contact lists, tagging photos, and sending invitations to join the site. It could be argued that the posting of information about ourselves and others has become normalized through our online experiences.

Given the unique properties of information once it is posted online, individuals have little control over who sees it, how it is interpreted, and how it will reflect on their reputation. To complicate matters further, people have no definitive way of knowing what information others have posted about them in the digital environment. Uploading others' information and images online is a one-click process, which typically does not require the person posting the information to obtain the subject's consent.

Real world risks of reputational harm

Much of the current conversation about online reputation focuses on awareness of potential risks and mitigation of any negative impacts that might occur. Reputational risks are often contextual, in that information that is appropriate in one context can be inappropriate in another context, where it can cause reputational harm. A common example would be party photos of intoxicated individuals that were shared among friends but end up being viewed by current or potential employers. For example, a U.S. teacher lost her job because of a holiday photo on Facebook showing her holding a glass of wine in one hand and a glass of beer in the other.[13]

With increasing frequency, online reputations factor into real-world decisions affecting individuals. For example, decisions such as the granting of credit or admission to an academic program may be made based on outdated, inaccurate or incomplete online information. To make matters worse, individuals are largely unaware of how online information may be limiting their opportunities because the decision-making process for many of these important decisions is currently not transparent.[14]

Reputation management services have long advised individuals to do regular searches on their names in order to be aware of negative search results and be in a position to mitigate reputational damage. Various strategies have been developed for "optimizing" search results so that positive results rise to the top. However, reputation management is a time-consuming and costly process requiring technical and/or financial resources that may be beyond the reach of the average person. Moreover, the increasing personalization[15] of the search process means that two individuals searching on the same name will likely get different results. This further complicates efforts to influence search results.

Once an online reputation has been tarnished by negative content, it is difficult to rehabilitate. The permanence of online information means that time does not erase past misdeeds and poor decisions. Following the 2011 Stanley Cup riots in Vancouver, law enforcement asked the public to provide photos and video, which they posted online and solicited the public's help in identifying suspects. The individuals identified as rioters may not have been ever charged or found guilty at all, and those who were actually convicted will continue to be associated with this event long after they have repaid their debt to society, potentially affecting many aspects of their lives, including future employability.

Posting information about others

Some websites are dedicated to publicizing personal information that people post about others. Among these are sites aimed at facilitating the exchange of information about professionals, such as doctors and professors. Other more insidious types of sites encourage the posting of sensitive personal information by people wanting to humiliate others for "entertainment" or revenge purposes, for example, so-called shaming sites of individuals who behave outside accepted social norms.[16]

Websites and other online services are structured to allow and sometimes even to encourage the posting of personal information about other individuals, for example, through the tagging of photos, uploading of contact lists, and posting comments. Obtaining consent from friends before we post their information rarely figures in the equation. Compounding the problem are search engines, which can find information with a few keystrokes.

A further example of how the architecture of online services impacts our reputations is the search engine autocomplete function. This is the algorithm that predicts the words individuals might enter as they type their search query, and suggests possible word combinations. Autocomplete has prompted litigation[17] in various jurisdictions in cases where the automated suggestions conveyed a derogatory or false characteristic about an individual. In recognition of this issue, Google has put in place a mechanism[18] allowing users to flag offensive auto complete suggestions for removal.

Under Canada's private sector privacy legislation, organizations must obtain the individual's consent to collect, use and disclose their personal information in the course of commercial activity, unless narrow exemptions apply. Individuals who post information in their personal capacity are not covered by private sector privacy laws.

A word about kids

Children and teens are particularly vulnerable when it comes to their online reputation. Not only are they themselves going online at a young age, their parents upload their photos and amusing anecdotes from their earliest days. Schools are requiring students to use digital technologies as part of the curriculum, and use of technologies by peers puts pressure on kids to conduct their social lives online. Research[19] has shown that children do not necessarily share personal information willingly but choose to do so in order to participate in social activities online.

These factors present a significant challenge to young people's ability to have control over their digital information and in turn their reputations. In their book *Born Digital*, Palfrey and Gasser[20] note in reference to a fictional 16 year old girl:

> *In the digital age, her social identity may be shaped by associations that are visible to onlookers at any moment through connections in social networks...In turn, the actions of her friends, and their shifting reputations, can affect her identity and her reputation.*

A further reputational risk is that childhood is a time of experimenting and testing boundaries. The permanence of digital information means that childhood transgressions or follies will remain findable and may have an effect on reputations for a long time to come. As the first digital generation grows up, it remains to be seen whether youthful patterns of behaviour will be affected by the knowledge that what we do as children will follow us for the rest of our lives. More generally, what will be the effects of a permanent record of our entire lives? Will a child who has a reputation as a bully be followed by that label through adulthood? Will it be possible to forget past mistakes? Will the increased risks to one's online reputation in this day and age ultimately affect behavior and the kinds of choices, and non-choices, that are made?

In an effort to respond to this problem, California passed a law called "*Privacy Rights for California Minors in the Digital World*,"[21] which requires companies, websites, and app developers to give kids under the age of 18 the option to delete information they themselves have posted. The law does not, however, cover information that others have posted about minors.

The right to be forgotten

Damage to reputation can be exacerbated when personal information that would otherwise have remained in the shadows is given prominence through search engines. In May 2014, the Court of Justice of the European Union (CJEU) ruled[22] that search engines must offer all Europeans the opportunity to request the removal of search results that link to information about them that is "inadequate, irrelevant, or no longer relevant." The decision came as a result of a case involving a Spanish man who objected when a Google search on his name returned links to newspaper stories mentioning past financial debts he had long since repaid. He believed those details about his life were no longer relevant but were affecting his reputation.

The CJEU's ruling is referred to as the "right to be forgotten" though in actual fact the information at issue is not deleted. The ruling affects only search engine results and allows the original information to remain on the website where it was posted. To reflect the fact that the offending information remains online, some commentators[23] have argued that instead of erasure, the CJEU ruling gives individuals a way of controlling access to their personal information by making it more difficult to find. In the words of Isabelle Falque-Pierrotin, the head of France's Commission nationale de l'informatique et des libertés (CNIL) as well as the Article 29 Working Party, the right to be forgotten "gives the possibility to each of us not to alter the past but to have the possibility to control a little bit what we have done in the past and their digital appearance."[24]

As of the writing of this paper, Google reported[25] receiving over 351,000 take-down requests covering over 1.2 million URLs. It removed links in almost 42% of cases. According to its website, Google takes into account a number of considerations in deciding whether to comply with a takedown request:

> *We must balance the privacy rights of the individual with interests that speak in favour of the accessibility of information including the public's interest to access to information, as well as the webmaster's right to distribute information. When evaluating requests, we will look at whether the search results in question include outdated or irrelevant information about the data subject, as well as whether there's a public interest in the information.*[26]

Google's process was informed by the Article 29 Working Party's guidelines for implementing the right to be forgotten decision, which includes considerations such as:

- Is the data subject a public figure?
- Was the content voluntarily made public by the data subject? Could the data subject have reasonably known that the content would be made public?
- Does the data have a disproportionately negative privacy impact on the individual?
- Does the search result link to information that puts the data subject at risk?

Google has been criticized[27] for not being more transparent about how it goes about balancing privacy with the public interest, as well as the lack of a recourse mechanism and independent oversight. Its role as the *de facto* decision-maker of these value-laden societal issues has been criticized by many. Google itself has admitted[28] to struggling with implementing the ruling and had convened an *Advisory Council to Google on the Right to Be Forgotten*[29] to gather expert opinions on how best to balance a person's right to be forgotten with the public's right to information.

The right to be forgotten should not be confused with the right to erasure under the EU General Data Protection Regulation.[30] The right to erasure requires the data processor to delete data if it is no longer required for processing, if the data subject has withdrawn consent, or if the processing violates any other provision of the Regulation. Unlike the right to be forgotten, which only affect search engines, the right to erasure places

responsibility on the organization that collects and processes the information in the first place and reinforces that organization's obligations under data protection law.

Recourse under PIPEDA

In Canada, no right to be forgotten or erasure laws exist *per se*. Individuals have been turning to the OPC for assistance when they come across websites that have posted their personal information without consent. The OPC oversees compliance with the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which sets out the rules that private-sector organizations must follow when they handle personal information in the course of their commercial activities. Generally, organizations cannot collect, use or disclose personal information without consent unless an exception to the requirement for consent applies. The law also gives individuals the right to access and to ask for corrections to personal information an organization may have collected about them. Individuals who believe an organization covered by PIPEDA is not living up to its responsibilities under PIPEDA have the right to file a complaint with the OPC.

The websites implicated by individuals who contact the OPC about reputational issues include dating sites, sites that re-post court and tribunal decisions, and, overwhelmingly, the so-called revenge and shaming sites.[31] One of the biggest challenges for the OPC in dealing with issues of online reputation has been asserting jurisdiction over the sites that come to our attention, particularly when they are based outside of Canada. In those circumstances, there may not always be a real and substantial connection to Canada, which is required in order for a foreign-based organization to be subject to PIPEDA. Moreover, in order for PIPEDA to apply, the website needs to be engaged in commercial activity. It is not unusual to find personal information posted without consent on websites set up for strictly personal use with no commercial purpose.

In cases where the OPC's jurisdiction was established, the Office has generally been successful in having information removed from organizations' websites. However, it is worth noting that once information has been posted online, there is never any guarantee that it has not been reposted elsewhere on the Internet. Despite removal on one site, the information may continue to reside on several other unknown sites.

One notable complaint under PIPEDA was against Globe24h, a Romanian-based website that republished court and tribunal decisions, including those from Canada. Globe24h had obtained the Canadian decisions by scraping a legitimate online court record repository that limits indexing of its decisions by individual name through search engines to minimize the privacy impact on individuals. By contrast, Globe24h allowed its reposted decisions to be indexed by search engines that surfaced personal information in response to searches on individuals' names. The site then charged individuals a fee to have their personal information taken down.

The OPC found that Globe24h contravened PIPEDA for collecting personal information without consent (and without an applicable exemption) and for an inappropriate purpose. The Commissioner stated in his finding,[32]

> *In our view, there is a significant difference between making court and tribunal decisions available online so that they are accessible to those who wish to consult past precedents and hold decision-makers accountable, and making those decisions – and their contents – indexable by popular search engines and available to anyone simply querying about another individual. As noted by the complainants in this case, indexing of court and tribunal decisions by search engines can provoke significant reputational harm and embarrassment to individuals by needlessly exposing sensitive personal information to inadvertent discovery.*

The Commissioner recommended to Globe24h that it delete from its servers the Canadian court and tribunal decisions that contain personal information and take the necessary steps to remove these decisions from search engine caches. Unfortunately, the company refused to implement those recommendations.

At the time of writing, an application was brought before the Federal Court under s.14 of PIPEDA against Globe24h. In an effort to minimize potential harm to individuals, the OPC reached out to some of the major search engines requesting they voluntarily remove links to the Globe24h website, or otherwise reduce the company's prominence in search results. We have seen some level of success in this regard.

In another case[33] investigated by the OPC involving reputational harm, a mother complained that someone had created a Facebook account in her teenaged daughter's name, who herself was not a Facebook user. The imposter contacted her friends and made inappropriate comments about them. The complainant approached Facebook about the impersonation, and upon confirming that the account was indeed fake, Facebook deleted it and all associated content (including the comments). The complainant wanted Facebook to go further and to inform all the individuals befriended by the imposter of the deception. While Facebook did not believe it would be appropriate for it to intervene in personal relations between individuals, it nonetheless agreed to institute measures to help mitigate the reputational consequences of impersonation for non-users of social networking sites, like the individual in this case. Facebook agreed to examine and investigate on a case-by-case basis matters of alleged impersonation of non-users that are brought to the site administrator's attention where the victim of an alleged impersonation requests a particular kind of assistance. Such assistance could include Facebook facilitating a process whereby non-users could themselves notify others who had been friended by an imposter account.

Other existing or potential forms of recourse

When discussing mechanisms that exist for deleting or correcting online information, it becomes apparent that the various parties involved, including organizations, legislators, technologists, educators and individuals, play a role in influencing how online reputations are shaped. The difficulty lies in determining relative levels of responsibility for an issue as amorphous as online reputation, and which engages other societal values such as freedom of expression, public interest, and historical integrity.

Organizations

a. Takedown policies

The most straightforward way to deal with personal information posted without consent is to ask the site to remove it. Organizations may agree to do this voluntarily. Many online services have long had in place policies and procedures for deleting an individual's own posts (e.g. Facebook, Twitter) when they no longer wish to have them on their personal page or account (although the information may have been reposted elsewhere or retweeted and be beyond the individual's control). Policies also exist for removing content that violates either the law or their terms of service. Traditionally, categories of content subject to removal include copyright infringements, defamatory information, and financial information such as credit card numbers.

More recently, in response to the growing problem of online abuse, some industry leaders have introduced mechanisms allowing users to request deletion of a wider range of content. For example:

- In its Terms of Service, Twitter bans users from posting "another person's private or confidential information" including "intimate photos or videos that were taken or distributed without the subject's consent."[34]
- Reddit amended its Privacy Policy to ban explicit images. As stated on its blog: "No matter who you are, if a photograph, video, or digital image of you in a state of nudity, sexual excitement, or engaged in any act of sexual conduct, is posted or linked to on Reddit without your permission, it is prohibited on Reddit. We also recognize that violent personalized images are a form of harassment that we do not tolerate and we will remove them when notified."[35]
- Facebook's Community Standards[36] guidelines explain the types of content banned from the service, such as bullying, harassment and nudity.

b. Intermediaries

Search engines are one of the primary tools for finding information online. Finding information through search engines has an aspect of serendipity – you do not know what you might find until you see the search results. If information is not indexed for a search engine search, retrieving it is much more difficult and generally involves looking at specific websites where the information is likely to be found or following links pointing to its location. In their paper "Obscurity and Privacy," Evan Selinger and Woodrow Hartzog state: "When information is hard to come by, the only people who will seize upon it are those with sufficient motivation to expend the

necessary effort and resources."[37] In other words, the person searching is making a conscious effort to unearth information and has probably made assumptions about what kind of information is likely to exist.

The concept of "privacy by obscurity," of making information harder to retrieve through search engines, figures prominently in online reputation management advice and services. For example, DeleteMe[38] will "remove your public profile from leading data sites" for US residents. Reputation.com offers a "Reputation Defender" service, whereby it will regularly scan the Internet and alert individuals when it finds their personal information.

Some reputation management services utilize principles of search engine optimization to help manage search results so that positive results appear first. Methods include flooding the Internet with new content about an individual in order to displace unwanted links to a lower spot in search results. (Ironically, this approach creates the paradox of giving up your privacy to protect your privacy.)

For their part, search engines have been very protective of the algorithms they use to index online information. It is known that sites can be deindexed, links to content can be removed, and the ranking of content in search listings can be made to rise or drop. For example, Google stated on its blog[39] "Our site quality algorithms are aimed at helping people find "high-quality" sites by reducing the rankings of low-quality content." The utility of such mechanisms in protecting online reputation merits further discussion.

As for the "right to be forgotten" debate, if such a mechanism were to be considered in Canada[40], there would need to be a careful balancing with other societal values, such as the right to freedom of expression, which is guaranteed under the *Canadian Charter of Rights and Freedoms*. While freedom of expression is already restricted in Canada by hate speech, obscenity, libel and defamation laws, freedom of expression remains a corner stone of Canada's democratic system, allowing individuals to express their opinions and ideas without interference or constraint by the government. In the digital realm, many of the measures used to control threats to privacy and reputation can also constrain freedom of expression. Threats to restrict free speech online have a chilling effect on people's willingness and ability to express themselves fully. At the same time, however, there is also a strong public interest in curbing the posting of personal information that is harmful and damaging to people's reputations particularly on a "net that never forgets."

The controversial decision by Twitter to block the accounts of Politwoops illustrates the complex issues at play. Politwoops is an online service that archives the deleted tweets of politicians in over 30 countries, including Canada, in the name of greater government transparency and accountability. After Twitter suspended Politwoops accounts for violating the terms of its Developer Agreement and Policy, there was an outcry[41] by prominent rights organizations such as the Electronic Frontier Foundation who argued that the public has a compelling interest in the expression of public officials.

Legislators

As online reputational harms become more widespread, legislators have been passing laws aimed at supplementing defamation laws and addressing specific online problems. For example, Russia's new "right to be forgotten law"[42] comes into effect in 2016. In the U.K., the posting of revenge porn recently became a criminal offence.[43] In the U.S., several states have passed laws prohibiting the online publication of booking photos (mugshots).

Many anti-cyberbullying measures address reputational harm resulting from the sharing of offensive comments and photos. For example, Bill C-13, the *Protecting Canadians from Online Crime Act*, introduced amendments to the *Criminal Code* to address the non-consensual sharing of intimate images and harassing communication. The Nova Scotia *Cyber-safety Act* allows for the prosecution of individuals who engage in the use of electronic communication "to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation."[44] In Manitoba, the proposed *Intimate Image Protection Act* would allow victims to pursue legal action and sue for damages in civil court.

Legislated retention periods might also provide some though limited relief. Under PIPEDA, organizations are allowed to retain personal information only as long as is necessary to fulfil the purpose for which it was collected. When it is no longer required, "information should be destroyed, erased or made anonymous."[45] This provision

is not particularly well suited for services that do not involve specific transactions that have an expected end date. For example, on a social media site, the purpose for collecting and processing information would continue to be fulfilled as long as an individual remained a member, however long that might be. Thus the retention provision might never be triggered.

In some industries, defined legislative limits are placed on retaining certain types of information. For example, in Canada negative credit information may only be retained[46] by credit reporting agency for six or seven years, depending on the province. As Julie Brill of the U.S. Federal Trade Commission suggested,[47] applying similar rules to other types of data would shorten the lifespan of online information. In turn, this could help limit the scope of online digital memory and reduce the amount of personal information available to affect an individual's reputation.

Another proposed solution for mitigating harm from online information involves disallowing decision-making on the basis of online information, as long as this does not harm other members of society. For example, several US states, including Montana and Connecticut, have enacted laws[48] prohibiting prospective employers from requiring candidates to provide their social media passwords. In Canada, provincial authorities such as the Ontario Human Rights Commission[49] and the British Columbia Office of the Information and Privacy Commissioner[50] have issued guidance to employers that using social media for background checks may put them in violation of provincial statutes that prohibit the collection and use of certain types of personal information.

Ryerson University Professor Avner Levin proposed,[51] as part of the OPC's Insights on Privacy Speaker Series, that online information should be off limits. In his view "action on its basis, by and large, would be prohibited, or would require additional, supportive information from other sources that would demonstrate that the action is based on other substantive grounds." Such an approach would, for example, prevent employers from terminating employment based on inappropriate online photos.

The Courts

Individuals who believe they have been maligned online have sued for defamation (libel) and sought an award of damages. Individuals have in some cases succeeded in revealing identities of anonymous perpetrators by subpoenaing ISPs for subscriber information linked to offending content in the context of a defamation lawsuit or potential lawsuit. For example, in *AB v Bragg Communications*[52], a teenaged girl was able to obtain a court order for the subscriber information associated with the IP address that had been used to create a fake Facebook profile of her using her photograph and to post offensive information about her and her sexual preferences. What is remarkable about this case is that the girl was able to obtain a partial publication ban on the outcome of the proceedings.

In Canada, defamation can sometimes constitute a criminal offence. For example, in an Ontario court case *R. v Simoes,*[53] a restaurant customer posted negative reviews about an Ottawa restaurant. In retaliation, the restaurant's owner began a harassment campaign that included setting up a false profile of the diner on a dating site and sent lewd e-mails to the customer's employer. The restaurant owner was convicted of defamatory libel under section 298 of the *Criminal Code*, and was sentenced to jail time.

Online harassment in the employment context could give rise to a human rights complaint if linked to a prohibited ground of discrimination, such as sexual harassment. In Canada, harassment can also sometimes constitute a criminal offence. Recently, there was a lengthy trial involving a man charged with criminal harassment after engaging in a Twitter-war with some political activists, following a disagreement about a videogame. If convicted, he could face a jail sentence.[54]

Privacy tort may provide recourse either by statute or at common law, such as the emerging tort of intrusion upon seclusion in Ontario[55]. Recently, the Quebec Superior Court found that a video recording of the plaintiff engaging in sexual activity with the defendant, which was made without the plaintiff's consent and which was

shared to a limited audience, was a violation of her right to privacy, and her honour and dignity, in contravention of both the Quebec *Charter of Human Rights and Freedoms* and the *Civil Code of Quebec*, and awarded significant damages. [56]

There are, however, significant limitations to judicial recourse. Defamation will not be found where the statements are true or constitute fair comment or responsible communication on matters of public interest; and defamation lawsuits do not address online reputational issues that involve damaging opinions and inappropriate photos, rather than untrue facts. Moreover, the purpose of pursuing recourse may be undermined as the offending information the individual wants hidden or forgotten is given further prominence through the litigation process, sometimes exacerbating damage to one's reputation. Further, the cost of pursuing litigation may not make this type of recourse accessible for everyone. In the criminal context, many cases do not result in charges or prosecutions, and those that do go to trial face a high burden of proof.

Finally, an important issue that the Courts grapple with in these cases is the tension between the constitutionally entrenched freedom of expression of the person making comments online and the interests of the individual who has allegedly been defamed or harassed, which makes these cases legally very complex.

Regulators

Since the Google Spain ruling, regulators have been increasingly seized with reputational issues related to search engines. In June 2015, the Article 29 Working Party published the results of a survey[57] to evaluate the practices of EU Data Protection Authorities (DPAs) with regard to requests for review of delisting decisions. The survey showed that over 2000 such requests had been submitted to EU DPAs in the first 18 months following the Google Spain ruling.

The scope of application of the Google Spain ruling outside the EU is currently being debated. France's CNIL is holding firm to its position[58] that the ruling requires search engines to remove URL links to all domains, not just on European geographical extensions. In the CNIL's opinion, if the information remains searchable under other Google domains, such as google.com, this would circumvent the very purpose of delisting and effectively strip the ruling of any meaning. Moreover, the CNIL believes that an individual's rights should not vary depending on the manner in which another individual queries a search engine. Google's position[59] is that the ruling is limited to Europe and does not apply to delisting from search results worldwide. Google is of the view that one region should not export its values and principles on other sovereign states that may have other views of the appropriate balance.

Technologists

No discussion of mechanisms for addressing online reputational risks would be complete without a mention of industry's role in protecting individuals' privacy and reputations through the design and infrastructure of online services. Proponents of "privacy by design" encourage technologists to build fair information principles into their products, so that the protection of personal information is integral to the running of online services.

Increasingly, the architects of technology are being reminded to consider the longer term societal impacts of their work. In a speech to technology professionals, danah boyd urged the audience "to consider the larger effects of their day-to-day activities on issues of fairness, privacy, politics and culture."[60] Christopher Parsons of the University of Toronto, in writing about how social bonds can be undermined in online social networks, calls for "technologists, legislators and citizens to advocate for basic transformation in the web's technical infrastructure."[61] In their paper about obscurity and privacy, Professors Evan Selinger and Woodrow Hartzog state: "design-based solutions could also be used to preserve or create obscurity, including (…) behavioural nudges that make obscurity practices salient and do not attempt to manipulate the user into engaging in obscurity-corrosive practices."[62] Oxford Professor Victor Mayer-Shönberger, a proponent of the "right to be

forgotten" advocates[63] for expiry dates on personal information so that individuals could choose what personal information to keep and what to let disappear over time.

There are obvious challenges in looking to industry to develop and adopt technological measures that effectively limit the amount of personal information available to support online business models that are predicated on monetizing personal information. However, when mitigating reputational risks is viewed through the lens of increasing consumer trust and building a competitive advantage, the benefits of pursuing solutions such as de-identification and anonymization become more compelling.

Individuals

During the OPC's Privacy Priority Setting discussions, the focus group participants we spoke with were aware of the reputational risks they face online, particularly in relation to employment opportunities and insurance coverage. We heard from Canadians that they take care to limit their digital footprint in order to protect their reputation. However, they expressed a lack of control over their reputations and concerns about the lack of mechanisms for taking information down.

According to a 2012 PEW Research Center study of US residents,[64] 44% of survey participants have deleted comments made by others on their profile and 37% have removed their names from photos that were tagged to identify them. These numbers reflect a concern about how posting by others affects our own reputation. Notably, the numbers do not capture the number of people who may have wanted to remove information posted by others but were unable to do so.

We heard during the OPC's Priority Setting Exercise that individuals have a responsibility for the information they post online and its consequences for online reputation. As for reputational damage caused deliberately, such as in cases of revenge porn, cyberbullying, and shaming sites, the same standards of ethical behavior that apply in the physical world should apply in the online environment as well. Users of technology should have a responsibility to behave ethically online and to respect others' privacy.

As alluded to earlier, the digital realm presents some specific challenges to protecting one's reputation. First, anyone with an Internet connection or a data plan has the means to create and distribute content, and find an instant audience. This democratization of information on the Internet means that anyone can be a movie maker, a restaurant critic, or a journalist without having their work pass through a quality control or legal compliance mechanism as it would if it were being published and distributed through traditional offline channels. Offensive content exists online in part because uploading it is seamless and taking it down is challenging.

What has been called the "online disinhibition effect"[65] contributes to a loosening of standards of behavior that govern social interactions offline. Generally speaking, the lack of face-to-face interaction feeds an attitude of anonymity whereby individuals feel less judged because the audience and they themselves seem invisible. As well, the act of uploading information feels removed from reality and lacking in the immediate feedback of observing others' reaction that would occur offline. Consequently, individuals feel freer to act out on their impulses when posting information about themselves or others.

Finally, in the offline world, things that are no longer relevant are gradually forgotten, but not so on the Internet. Vast stores of digitized information can be easily searched to reveal past indiscretions that can affect lives today in unanticipated ways. Individuals cannot rely on the passage of time to erase embarrassing moments. These challenges to protecting and preserving one's online reputation bring urgency to the need for online ethics and to reinforcing the notion that users of technology should respect others' privacy

Educators

Cyber ethics and empathy for others online are an integral part of the digital literacy education currently being integrated into school curricula. For example, the *Raising Ethical Kids for a Networked World* tutorial[66] developed by MediaSmarts, the leading Canadian media and digital literacy organization, focuses in part on respecting people's personal information by not oversharing.

Psychologist Sherry Turkle said “Technology is making a bid to redefine human connection -- how we care for each other, how we care for ourselves – but it's also giving us the opportunity to affirm our values and our direction.”[67] One can hope that digital literacy education will help contribute to building a culture of empathy where revenge porn, cyberbullying and shaming sites are not tolerated, and that the posting of others’ information without permission will someday be considered outside the social norm.

Digital literacy has been an area of focus for the OPC, particularly on youth privacy issues. Under the OPC’s Contributions Program, we have funded initiatives such as the “Privacy Educational Kit for Teachers and Students”[68] and “Privacy Pirates: An app on online privacy.”[69] As part of our youth outreach efforts, the OPC is developing tools and resources to help young people better understand how digital traces are created and their potential impact on their reputation and the reputations of others. To date, the OPC has created a short video entitled *Information: Once it’s out there….,* meant to encourage young people to think of the consequences of sharing too much information online. The OPC will be developing a lesson plan to accompany the video which would focus on risks and strategies to prevent reputational harm.

The British Columbia (B.C.) Representative for Children and Youth, together with the B.C. Information and Privacy Commissioner, in their 2015 report on cyberbullying,[70] identify digital education as an integral part of the effort to address cyberbullying. In their opinion, young people need to be taught the value of privacy to citizenship and democracy so that they are able to make responsible decisions as members of society as a whole.

Conclusion

A section of the OPC’s 2012 Annual Report was devoted to raising awareness about online reputation. We said “Information in the online universe is highly pervasive and accessible. It is generally also persistent, outlasting all but the most determined efforts to control it. When such information is damaging or wrong, it can pose a grave threat to a person’s privacy and reputation – online as well as in the physical world.”

When it comes to the potential effects of information we and others post about us, reputational damage can occur without much effective recourse. The fact that most laws predate social media may account for the gaps in legal coverage. Nevertheless, other means of addressing this issue, for example through industry codes of practice or technological measures, could prove to be part of the solution.

The search for solutions and for transposing physical world ethical rules to the virtual world is not without challenges. Commentary opposed to the CJEU’s right to be forgotten decision has focused on its potential to chill free speech and authorize censorship. Internet infrastructure, particularly the ease of posting information as well as its permanence in the absence of any universal governance process, is also cited as a barrier to solutions. Moreover, there are significant legal questions still to be answered, for example, does PIPEDA currently recognize certain aspects of the right to be forgotten through concepts such as accuracy, appropriate purpose, or the right to withdraw consent? Or, would PIPEDA need to be amended to address these questions more squarely?

Our aim in publishing this paper is to draw attention to this emerging challenge in privacy protection with the intention of stimulating discussion about solutions. Ultimately, we intend to develop a position on remedies. To this end, we are calling on individuals, organizations, academics, advocacy groups, information technologists, educators and other interested parties to propose new and innovative ways to protect reputational privacy as a follow-up to this discussion paper. We invite essays to answer one (or more) of these five questions:

- We have highlighted some potential gaps in protections between the online and offline worlds. What other gaps exist?
- What practical, technical, policy or legal solutions should be considered to mitigate online reputational risks?

- Can the right to be forgotten find application in the Canadian context and, if so, how?
- Should there be special measures for vulnerable groups?
- Who are the key players and what are their roles and responsibilities?

Please refer to the call for submissions for more information.

Additional Resources

The following is a list of resources that delve in more detail into topics raised in this paper.

Austin, L. "Privacy and Private Law: The Dilemma of Justification" In: *McGill Law Journal*, vol. 55, n. 2, 2010, pp. 165-210. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2016969

Bazelon, Emily. 2013. *Sticks and Stones: Defeating the Culture of Bullying and Rediscovering the Power of Character and Empathy*. Random House Trade Paperbacks.

Beasley, Berrin and Mitchell Haney, ed. 2013. *Social Media and the Value of Truth*. Lexington Books.

Citron, Danielle. 2014. *Hate Crimes in Cyberspace*, Harvard University Press.

Dash, Anil. July 24, 2014. "What is public?" Online at https://medium.com/message/what-is-public-f33b16d780f9

Hartzog, Woodrow and Frederic Stutzman *Obscurity by Design.* In: Washington Law Review, June 2013. Online at http://privacylawsalon.com/wp-content/uploads/2014/01/Hartzog-Stutzman-Obscurity-by-Design.pdf

Hartzog, Woodrow and Frederic Stutzman. *The Case for Online Obscurity*. In: California Law Review, February 2013. Online at http://www.californialawreview.org/wp-content/uploads/2014/10/01-HartzogStutzman.pdf

Ivester, Matt. 2011. *Lol…OMG*! Serra Knight Publishing.

James, Carrie. 2014. *Disconnected: Youth, New Media, and the Ethics Gap*. The MIT Press.

Levmore, S. and MC. Nussbaum. ed. 2010. *The Offensive Internet: Privacy, Speech and Reputation*. Harvard University Press. Specifically, these essays:

"The Internet's Anonymity Problem" by Saul Levmore
"Believing False Rumours" by Cass R. Sunstein
"Reputation Regulation: Disclosure and the Challenge of Commensurating Computing" by Frank Pasquale

Lewinsky, Monica. "The Price of Shame." TED Talk. March 2015. Online at http://www.ted.com/talks/monica_lewinsky_the_price_of_shame?language=en

Marwick, A. and R. Miller. June 10, 2014: *Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape*. Centre for Law and Information Policy at Fordham Law School. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447904

Massum, Hassan and Mark Tovey. ed. 2011. *The Reputation Society: How Online Opinions are Reshaping the Offline World.* The MIT Press.

Mayer-Shönberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press.

Morozov, Evgeny. 2013. *To Save Everything Click Here: The Folly of Technological Solutionism.* PublicAffairs.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Potts, D.A. 2011. *Cyberlibel: Information Warfare in the 21st Century?* Irwin Law Inc.

Solove, Daniel J. 2007. *The future of reputation: gossip, rumor, and privacy on the internet*. Yale University Press.

Trottier, D., 2014. *Identity Problems in the Facebook Era*.: Routledge.

Tunick, Mark. 2015. *Balancing Privacy and Free Speech: Unwanted attention in the age of social media*. Routledge.

West Coast LEAF. *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*. June 2014. Online at http://www.westcoastleaf.org/userfiles/file/Cyber%20Misogyny%20Report.pdf.

Notes

[1] William Shakespeare, *Othello* (c. 1603), (Iago) Act II, scene 3, line 268.

[2] Deborah G. Johnson, Priscilla M. Regan and Kent Wyland. "Campaign Disclosure, Privacy and Transparency." *William & Mary Bill of Rights Journal*, Vol, 19, Issue 4, Article 7, 2011. Online at http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1585&context=wmborj.

[3] Oxford Dictionaries. Online at http://www.oxforddictionaries.com/definition/english/reputation.

[4] Erving Goffman.1959. *The Presentation of Self in Everyday Life*. Anchor Books.

[5] danah boyd. 2010. "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications." In *Networked Self: Identity, Community, and Culture on Social Network Sites* (ed. Zizi Papacharissi), pp. 39-58.

[6] Deborah G. Johnson, Priscilla M. Regan and Kent Wayland. "Campaign Disclosure, Privacy and Transparency." *Wiliam & Mary Bill of Rights Journal*, Vol, 19, Issue 4, Article 7, 2011. Online at http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1585&context=wmborj.

[7] The Guardian. "American family's web photo ends up as Czech advertisement." June 11, 2009. Online at http://www.theguardian.com/media/2009/jun/11/smith-family-photo-czech-advertisement.

[8] The Citizen. "Genetic testing company's use of child's image outrages mother Christie Hoos." June 18, 2015. Online at http://www.cbc.ca/news/canada/british-columbia/genetic-testing-company-s-use-of-child-s-image-outrages-mother-christie-hoos-1.3118339.

[9] Official Google blog. "Eye-tracking studies: more than meets the eye." February 6, 2009. Online at http://googleblog.blogspot.ca/2009/02/eye-tracking-studies-more-than-meets.html.

[10] Chitika Online Advertising Network. "The Value of Google Result Positioning." June 7, 2013. Online at http://chitika.com/google-positioning-value.

[11] A term coined by Professor Nicolaus Mills in his commentary on reality television: "Television and the Politics of Humiliation," Dissent (00123846), Summer 2004, Vol. 51 Issue 3, p. 79.

[12] Given the nature of this case, we have chosen to not provide a specific reference.

[13] CBS News, *"Did the Internet Kill Privacy?"* February 6, 2011. Online at http://www.cbsnews.com/news/did-the-internet-kill-privacy/.

[14] In recognition of this issue, the Office of Technology Research at the Federal Trade Commission's Bureau of Consumer Protection is focusing on algorithmic transparency with the aim of ensuring algorithms do not result in harmful or discriminatory effects on consumers. For more information see https://www.ftc.gov/news-events/blogs/techftc/2014/12/hello-world.

[15] Results returned by many search engines are tailored to the individual based on a variety of factors, such as location and search history.

[16] We have chosen not to identify any of these sites in order to not give them unwarranted prominence.

[17] Stavroula Karapapa and Maurizio Borghi. "Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm." *International Journal of Law and Information Technology*, 2015, 23, pp. 261–289. July 2015. Online at http://ijlit.oxfordjournals.org/content/23/3/261.full.pdf +html

[18] Google Search Help: Autocomplete. Online at https://support.google.com/websearch/answer/106230?hl=en.

[19] Jacquelyn Burkell, Valerie Steeves & Anca Micheti, *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand.* 2007. Online at www.idtrail.org/files/broken_doors_final_report.pdf.

[20] Palfrey, J. and U. Gasser. 2008. *Born Digital: Understanding the First Generation of Digital Natives*, New York: Basic Books.

[21] *Privacy Rights for California Minors in the Digital World*. Online at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

[22] Court of Justice of the European Union, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014), Case 131/132. Online at http://curia.europa.eu/juris/document/document.jsf?docid=163494&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=111438.

[23] Eric Posner. "We all have the right to be forgotten." Slate. May 14, 2014. Online at http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html.

[24] Mark Halper. "Isabelle Falque-Pierrotin: Privacy needs to be the default not an option." Wired. June 2015. Online at http://www.wired.com/2015/06/isabelle-falque-pierrotin-privacy-needs-default-not-option/

[25] Google transparency report, December 15, 2015. Online at http://www.google.com/transparencyreport/removals/europeprivacy/.

[26] Letter from Google to the Article 29 Working Party. July 31, 2014. Online at https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit?pli=1.

[27] Medium. "Open letter to Google from 80 Internet scholars: Release RTBF compliance data." May 13, 2015. Online at https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

[28] Computerworld. "This is how Google handles 'Right to be forgotten' requests." Nov. 19, 2014. Online at http://www.computerworld.com/article/2849686/this-is-how-google-handles-right-to-be-forgotten-requests.html.

[29] Online at https://www.google.com/advisorycouncil/.

[30] European Parliament. "Proposed General Data Protection Regulation." March 12, 2014 version. Online at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

[31] These account for over half of complaints and inquiries the OPC has received to date about non-consensual posting of personal information.

[32] "Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA." (PIPEDA Report of Findings 2015-002). OPC website. Online at https://www.priv.gc.ca/cf-dc/2015/2015_002_0605_e.asp.

[33] "In response to a case of a teen who was a victim of online impersonation, Facebook agrees to help non-users, on a case-by-case basis, reinstate their on-line reputation." (PIPEDA Report of Findings 2013-010). OPC website. Online at https://www.priv.gc.ca/cf-dc/2013/2013_010_0711_e.asp.

[34] "Private Information Posted on Twitter." Twitter Help Center. Accessed on July 6, 2015 at https://support.twitter.com/groups/56-policies-violations/topics/236-twitter-rules-policies/articles/20169991-private-information-posted-on-twitter#.

[35] "Protecting your digital privacy." reddit blog. February 24, 2015. Accessed on July 6, 2015, at http://www.reddit.com/r/announcements/comments/2x0g9v/from_1_to_9000_communities_now_taking_steps_to.

[36] Facebook Community Standards. Accessed on July 6, 2015, at https://www.facebook.com/communitystandards.

[37] Evan Selinger and Woodrow Hartzog. "Obscurity and Privacy." In: Routledge *Companion to Philosophy of Technology*. 2014. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866

[38] Abine website. www.abine.com/deleteme/landing.php.

[39] Google webmaster central blog. "More guidance on building high-quality sites." May 6, 2011. Online at http://googlewebmastercentral.blogspot.ca/2011/05/more-guidance-on-building-high-quality.html.

[40] Some provincial jurisprudence is developing in the area of de-listing search results. For more information , please refer to *Equustek Solution Inc. v. Jack,* (2014 BCSC 1063) and *Niemela v. Malamas (2015 BCSC 1024).*

[41] Accessnow website. "Open letter to Twitter to restore Politwoops access to API." September 2015. Online at https://www.accessnow.org/pages/open-letter-twitter-restore-politwoops-access-api.

[42] http://www.natlawreview.com/article/right-to-be-forgotten-russian-data-protection-law-has-passed-all-stages-approval.

[43] The Telegraph. "Revenge porn: new offence comes into force." April 12, 2015. Online at http://www.telegraph.co.uk/news/uknews/crime/11530889/Revenge-porn-New-offence-comes-into-force.html

[44] *Cyber-Safety Act*, SNS 2013, c 2. Online at http://www.canlii.org/en/ns/laws/stat/sns-2013-c-2/latest/sns-2013-c-2.html

[45] Principle 4.5.3 of PIPEDA.

[46] Financial Consumer Agency of Canada. "Understanding your Credit Report and Credit Score." Online at http://www.fcac-acfc.gc.ca/Eng/resources/publications/creditLoans/Pages/Understa-Comprend-7.aspx.

[47] Evan Selinger and Woodrow Hartzog. "Why you have the right to obscurity." The Christian Science Monitor. April 15, 2015. Online at http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0415/Why-you-have-the-right-to-obscurity.

[48] National Conference of State Legislatures. "*Access to Social Media Accounts and Passwords*." September 14, 2015. Online at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

[49] Ontario Human Right Commission Facebook page post dated March 23, 2012. Online at https://www.facebook.com/the.ohrc/posts/320570581329371.

[50] Office of the Information and Privacy Commissioner of British Columbia. "*Guidelines for Social Media Background Checks*." October 2011. Online at https://www.oipc.bc.ca/guidance-documents/1454

[51] Avner Levin. "Should Online Information be a Prohibited Ground." OPC's Insights on Privacy Speaker Series, March 2011. Online at https://www.priv.gc.ca/information/research-recherche/2011/levin_201103_e.asp.

[52] In A.B. v. Bragg Communications Inc., 2012 SCC 46, [2012] 2 S.C.R. 567, the Supreme Court of Canada overturned the lower court rulings and allowed the plaintiff to obtain the order anonymously. A.B. v. Bragg Communications Inc., [2012] 2 SCR 567, 2012 SCC 46 (CanLII), <canlii.ca/t/fstvq>.

[53] There is no published lower court decision. The Ontario Court of Appeal upheld the lower court's conviction, but reduced the jail sentence. R. v. Simoes, 2014 ONCA 144 (CanLII), <canlii.ca/t/g469m>.

[54] R. v ELLIOTT, GREGORY A. (Ontario Court). The verdict is expected to be released in January 2016.

[55] *Jones v. Tsige*, 2012 ONCA 32.

[56] *L.D. c. J.V*. [2015] JQ no 2563, 2015 QCCS 1224.

[57] Press Release Issued by the Article 29 Working Party, June 18, 2015. Online at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20150618_wp29_press_release_on_delisting.pdf.

[58] CNIL. "Right to delisting: Google informal appeal rejected." September 21, 2015 Online at http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/.

[59] Google Europe Blog. "Implementing a European, not global, right to be forgotten." July 30, 2015. Online at http://googlepolicyeurope.blogspot.ca/2015/07/implementing-european-not-global-right.html.

[60] "Teens are waging a privacy war on the Internet – Why marketers should listen." University of Pennsylvania: Wharton website. August 5, 2014. Online at http://knowledge.wharton.upenn.edu/article/teens-privacy-online.

[61] Christopher Parsons. "Sex, Lies and Digital Memory: How Social Surveillance Threatens Communities." In: *Communication in Question: Competing Perspectives on Controversial Issues in Communication Studies.* Nelson Education, 2013, pp. 174-180.

[62] Evan Selinger and Woodrow Hartzog. "Obscurity and Privacy." In: Routledge *Companion to Philosophy of Technology*. 2014. Online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866.

[63] Viktor Mayer-Schönberger. "Why we need to let our online memories go." *The Washington Post*, November 23, 2012. Online at https://www.washingtonpost.com/opinions/why-we-need-to-let-our-online-memories-go/2012/11/23/29d0e54e-33ec-11e2-bfd5-e202b6d7b501_story.html.

[64] Mary Madden. PEW Internet and American Life Project. "Privacy management on social media sites." February 24, 2012. Online at http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/.

[65] John Suler. CyberPsychology & Behavior. June 2004, 7(3): 321-326. Online at http://online.liebertpub.com/doi/abs/10.1089/1094931041291295.

[66] Online at http://mediasmarts.ca/tutorial/raising-ethical-kids-networked-world.

[67] Sherry Turkle. "Connected but alone" TED Talk, Feb 2012. Online at http://www.ted.com/talks/sherry_turkle_alone_together.

[68] For more information, see https://www.priv.gc.ca/resource/cp/2013-2014/p_201314_05_e.asp.

[69] For more information, see https://www.priv.gc.ca/resource/cp/2014-2015/p_201415_05_e.asp.

[70] Office of the Privacy Commissioner for British Columbia, Representative for Children and Youth. "Cyberbullying: Empowering children and youth to be safe online and responsible digital citizens." November 2015. Online at http://www.rcybc.ca/sites/default/files/documents/pdf/reports_publications/rcy_cyberbullying-web.pdf.