Submission to Consultation on Online Reputation

Prepared for the Office of the Information and
Privacy Commissioner of Canada

April 28, 2016

BC Freedom of Information and Privacy Association
103 – 1093 West Broadway
Vancouver, British Columbia, V5N 1E2
Phone: 604-739-9788 | Fax: 604-739-9148
fipa@fipa.bc.ca

FIPA would like to acknowledge the Law Foundation of British Columbia. Their ongoing support of our work in the areas of law reform, research and education makes submissions like this possible.

Introduction

FIPA is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform.

We thank the Office of the Privacy Commissioner of Canada for this opportunity to discuss issues relating to online reputation.

While this submission focuses on informing the OPC's development of a policy position on the issue of online reputation, it also contains discussions that could be applied to regulators more generally, as well as to industry and government.

We have read and understood the consultation procedures in the Notice of Consultation and Call for Essays, and we hope you will find this submission helpful.

Summary

In this submission, FIPA considers what policies will best allow Canadians to have control of information about them, prevent and reduce information-based harm, and ensure reputational privacy enhances—and does not impede—free association and democratic free expression.

We look first at existing protections – from the law to social norms, and from market solutions to online architecture. We argue that existing privacy statutes, the common law and statutory torts, and *Criminal Code* provisions already go some way toward protecting individuals' ability to govern the use of their personal information and image, but that legislation cannot solve all of our societal problems.

We talk about normative constraints reinforced largely through informal peer-to-peer education, which allow individuals to share information discriminately in quasi-public settings. But those norms are still being developed and learned.

We discuss privacy protections in the architecture of social networks and other sites – but point out that privacy controls vary and can change, and can leave less technologically-sophisticated users behind.

And we talk about market solutions that exist to solve reputational woes – but only for those who can pay.

To help solve fill some of the gaps in the existing protections, we propose (1) public education that takes a rights-based approach to online reputation; (2) higher standards for privacy controls, including privacy-protective default settings, that social networking companies could agree to; and (3) legal solutions that do not overreach, and specifically legislate against unwanted behavior.

This submission also talks about "obscurity"— defined as a lack of search visibility, unprotected access, identification, or clarity—and practical ways to make use of the concept, before delving into the question of a "right to be forgotten".

We urge great caution in implementing the latter—we argue against intermediary liability, warn against creating tiered access, and urge insurance against erroneous or malicious requests, among other things—and make four broad recommendations:

- That any measures taken to address online reputation concerns be handled by an appropriately-resourced body that is accountable to the public.
- That any obscuring or takedown processes be relatively simple, have clear evaluation criteria, and involve the notification of content creators or hosts when appropriate
- That public education efforts should be made so that Internet users know that information may be omitted from their searches or browsing.
- That data should be collected about online reputation's effects on the online and offline lives of individuals.

We hope you will find our discussion useful.

Overview

What does online reputation mean for Canadians?

For many of us, it's what potential employers could learn, with little effort, by simply typing a name into a search engine and pressing "enter". It's also what family, friends, romantic partners, or acquaintances could learn by doing the same, or by connecting through an online social platform. In the future, it may be what complete strangers are able to find out by scanning someone's face through a pair of smart glasses, like Google Glass.

For our youth, online reputation can paint a picture of growing pains. For some it will be a link to an endearing, albeit somewhat-embarrassing past; for others it will be a haunting tie to childhood teasing, bullying, or even abuse, which may otherwise have been eventually left behind.

Vulnerable groups—such as people with disabilities or with a medical condition, visible minorities, survivors of violence or abuse, and LGBTQ people, among many other groups—may find that control of their online reputation can allow them to reach into spheres that would otherwise be more difficult to enter, or to find one another and create communities, or to effectively publicize their experiences and advocate for change – or that a lack of control can brand them as outsiders.

The online reputations of our politicians and policy makers can be used to make more informed decisions and to hold people in power to account, though some would argue that too much information—information that is too personal, or with too little context, for example—can have the opposite outcome, and can distract us from important issues and unfairly subject these individuals to personal, rather than professional, scrutiny.

The online world is an extension of the offline. In it, information flows easily through time and space. When we write or speak, we broadcast and create records.

For better or for worse, our audience can expand quickly without our consent, and what would once have been casual or ephemeral can quickly become serious, permanent, and retrievable by anyone. But this is mitigable. When laws are broken, takedowns can be ordered; otherwise, measures to create obscurity can be taken.

In this submission, we will discuss some of the considerations we must make when we discuss the mitigation of online reputational risks, and the rights and interests we must seek to balance.

Outcomes

Let's begin with a discussion of the values we want to advance and protect when creating any policy that affects information flows.

In *Privacy as Contextual Integrity*, Helen Nissenbaum describes three outcomes that privacy policies typically strive for: "(1) limiting surveillance of citizens and use of information about them by agents of government, (2) restricting access to sensitive, personal, or private information, and (3) curtailing intrusions into places deemed private or personal." In Canada, these principles have largely been addressed in positions taken by the Office of the Privacy Commissioner,[1] among others.

For the mitigation of online reputational risks, however, we must add to these. We must consider what policies will best allow Canadians to have control of information about them, and to be empowered to autonomously make decisions about what they wish to share and with whom they wish to share it. We must consider how to prevent and reduce information-based harm, especially for vulnerable groups, and how to prevent reputation information from reinforcing social and economic inequality. And, in a time when interpersonal communication often takes place on nonymous social platforms, we must ensure that reputational privacy serves to enhance—and not impede—free association and democratic free expression.

Often we are asked to strive to balance privacy rights and interests with values such as freedom of speech and of the press, economic vitality (especially that of the digital economy), and security. However it is our view that these values need not be compromised.

Privacy and participation are not oppositional values; they can be mutually reinforcing. Selective privacy and anonymity can create the environment necessary for important information to be shared with journalists or directly with a wider public. As we've seen through developments in privacy by design,

[1] The OPC's arguments against the *Anti-Terrorism Act*, for example, pushed back against an expansion of unchecked government surveillance; a search for "sensitive information" (without quotes) on the OPC website yields approximately 1161 results.

authentication can exist without identification.[2] And privacy can serve to enhance security measures and encourage participation in the digital economy.

A right to control one's reputation online should not come at the expense of the right of free expression or the freedom of the press. Takedowns or measures to create obscurity should always be weighed against the author's or public's interest in the information in question – concealing or removing information from the Internet are not actions that should be taken lightly. In addressing reputational privacy Canada must take a well-reasoned, transparent approach to ensure the interests of content creators, publishers, and hosts are taken into account alongside the autonomy, safety, and comfort of the individuals about whom information is shared.

Existing protections

There are many existing protections that serve to prevent or mitigate online reputational harm and its effects. These are not limited to provisions in the *Criminal Code* or privacy laws—though these are significant forces for preventing and mitigating online harassment, extortion, and abuse—but also include social norms (and public education), market solutions (such as reputation management), and architecture-based solutions (such as platforms' privacy settings). [3] In the following section, we will discuss some of these solutions.

Legal protections

In Canada, privacy laws including the *Privacy Act*, *the Personal Information Protection and Electronic Documents Act (PIPEDA)*, and various provincial privacy laws protect individuals' ability to govern the use of their personal information and image. An August 2014 "Technology Bulletin" from McMillan LLP outlines some of the existing protections in privacy law:

> *"Private sector companies cannot disclose personal information without consent unless it can be proven there is a legitimate public interest right to know. Individuals also have the right to expect any publication of their personal information to be accurate, complete and up-to-date. Consequently, PIPEDA gives individuals the right to request their online information removed by the original publisher if their consent is not given or if the information is not up-to-date."* [4]

---

[2] For example, in *Transparent Lives: Surveillance in Canada*, authors describe a privacy-respecting biometric system used to control access to the Port of Halifax, in which an infrared scan of the back of the cardholder's hand is embedded in a smart card. The biometric is stored only on the individual card, and not in a database. A worker is able to access secure areas of the port by scanning both the card and the back of their hand – something that is done anonymously, but securely. This has been touted as an example of successful privacy by design in real-world authentication systems.

[3] Lawrence Lessig's *Code and Other Laws of Cyberspace* details these constraints, and describes how norms, markets, architectures, and laws work interdependently to regulate behaviour, online and off.

[4] *The Internet Never Forgets: Google Inc.'s "right to be forgotten" EU ruling and its implications in Canada*. August 2014. McMillan Technology Bulletin. http://www.mcmillan.ca/The-Internet-Never-Forgets-Google-Incs-right-to-be-forgotten-EU-ruling-and-its-implications-in-Canada

Certain torts—defamation, but also torts such as the Ontario common law tort of public disclosure of private facts, and the BC statutory tort of using someone's name or portrait without license for the purpose of advertising or promoting the sale of a property or service—also make actionable activities that cause reputational harm.

The *Criminal Code of Canada* also has several provisions that can be applied in serious cases of online reputational harm. In their joint report on cyberbullying, the Office of the Information and Privacy Commissioner of BC and the Representative for Children and Youth of BC identify a number of offences that may apply to extreme cyberbullying activities,[5] which may also apply to online reputation harm and some effects thereof:

- *criminal harassment (s. 264)*
- *uttering threats (s. 264.1)*
- *intimidation (s. 423(1))*
- *defamatory libel (s. 298-301)*
- *assault (s. 265-273)*
- *mischief in relation to data (s. 430 [1.1])*
- *unauthorized use of computer (s. 342.1)*
- *identity fraud (s. 403)*
- *extortion (s. 346)*
- *false messages, indecent or harassing telephone calls (s. 372)*
- *counselling suicide (s. 241)*
- *incitement of hatred (s. 319)*
- *child pornography offences (s. 163.1) and*
- *the non-consensual distribution of intimate images (s. 162.1)*

The cyberbullying report makes it clear, however, that criminal law alone cannot be relied upon to deter unwanted behaviour, especially as its application must be balanced with the *Charter* right to freedom of expression. The report recommends that legal responses be regarded as one of a number of pieces of a strategy to promote respectful online interaction. “Essentially,” the report states, “responsible and respectful behaviour cannot be legislated.”

We are entering an era where the law of defamation—which has been the preserve of the moneyed and the well-known public figures fighting those who speak ill of them—is now affecting many more people who are in no way public figures. Processes and remedies that were developed in the past will have to be updated to recognize this new reality, or new processes and remedies will have to be developed.

[5] Office of the Information and Privacy Commissioner for British Columbia and the Representative for Children and Youth. November 2016. *Cyberbullying: Empowering children and youth to be safe online and responsible digital citizens*. https://www.oipc.bc.ca/special-reports/1882

Norms

Especially in the cases of peer-to-peer discussions and sharing on social media, social norms are a key regulator. Lessig defines social norms succinctly as "normative constraints imposed not through the organized or centralized actions of a state, but through the many slight and sometimes forceful sanctions that members of a community impose on each other."[6]

In an article posted on Medium.com, popular blogger Anil Dash posits that so-called 'public' speech on social media is akin to a private conversation in a public setting.[7] He compares posting to Facebook or Twitter to speaking quietly at a restaurant, or near an open window in one's home. He is far from alone in this understanding of social media.

Danah boyd has studied teenagers' and college students' use of online communication channels, and has found this to be a common understanding of social media communications among youth.[8] But the online world does introduce complications, and blurs some of the lines between privacy and publicity. Offline, she writes,

> *"When we share updates about our lives over coffee, we don't expect our interlocutors to share them widely, because 1) we don't believe that said information is interesting enough to be spread widely; 2) it's difficult to disseminate social information to a large audience in face-to-face contexts; and 3) recording a conversation or sharing every detail of an interaction would violate both social norms and the trust assumed in a relationship."* [9]

In the case of the online world, however, boyd argues, "in an era of social media where information is often easily accessible, it's all too easy to conflate accessibility with publicity."

But online, one can still speak to a particular audience, participate on platforms that prevent unintentional broadcast, and erase or obscure records as needed. And informational norms still govern behaviour.

Helen Nissenbaum identifies two key categories of information norms that apply: norms of appropriateness and norms of flow or distribution.[10] Norms of appropriateness dictate what information about a person is appropriate, or fitting, to reveal in a particular context; norms of distribution dictate how information may move or be transferred from one party to others after it has been revealed.

---

[6] Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace.* p.340
[7] Dash, Anil. *What Is Public?* July 2014. https://medium.com/message/what-is-public-f33b16d780f9#.mb1o26191
[8] See, for example, Marwick and boyd's *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*
[9] Boyd, danah and Alice Marwick. May 2011. *Social Steganography: Privacy in Networked Publics.* http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf
[10] Nissenbaum, Helen. 2004. Privacy as Contextual Integrity.

Nissenbaum's theory of privacy as contextual integrity proposes that "privacy violations occur when the disclosure of one individual's personal information by another disrespects the context in which the information is disclosed."

Norms such as these can be shaped by architecture and law, to some degree, but are reinforced largely through informal peer-to-peer education, where social inclusion or exclusion depends on one's ability to understand and adhere to communication norms. This is largely effective—allowing individuals to share information discriminately even within open architectures—and contribute to a reasonable expectation of obscurity when it is, as Lior Strahilevitz writes, "theoretically possible, but extraordinarily unlikely, that information shared with a few individuals will ultimately become widely known by the public."[11]

Norms go a long way to protecting online reputation on a peer-to-peer level, but as Marshall McLuhan famously stated, "we are always living ahead of our thinking." The structure of online discourse changes frequently, and social norms are not always quick to adapt.

As well, these norms do not necessarily apply universally—they vary between cultures and even between particular social groups—and when businesses are involved in the publishing or publicizing of information, norms are simply not enough.

Architecture

Control of one's online reputation is affected not only by what information-sharing is considered socially appropriate, but by what is structurally feasible.[12] Online, permanence and searchability are the default, physical distance is not a factor, and broadcasting to a wide audience is easier than ever. However, the architecture of the online spaces, or platforms, where people participate online can dramatically differ.

With online banking, for example, one should be able to expect total privacy. No information is meant to be shared with others, and privacy is maintained through password protection and the absence of indexing for search.

With social media, on the other hand, where the intended audience and the size thereof can vary greatly, adjustable privacy settings are key.

This goes beyond the decision of whether to participate anonymously—though anonymity or the use of aliases can be a useful control as well. Social media interactions are often rooted in real-life social networks, and individuals will use (and are sometimes forced to use) their real names to facilitate these interactions. Individuals also choose to use their real names as a means of controlling their broader online reputation, allowing it to be based more on what they say than what is said about them. This "nonymous social web" is where privacy settings become most important.

[11] See Lior Strahilevitz's "Social Networks Theory of Privacy"
[12] Boyd, danah and Alice Marwick. May 2011. *Social Steganography: Privacy in Networked Publics.*

Jurgenson and Rey point out that the availability of privacy controls encourages sharing, and that evidence suggests those who share are generally the most sensitive to privacy settings.[13] They quote a Pew survey that indicates that as early as in 2010, 65% of adult American social media users adjusted the privacy settings on their profiles,[14] and in 2012 81% indicated they knew how to "manage the capture of their data" be it through privacy settings, browser settings, or otherwise.[15]

Users' understanding and control of privacy settings are an important way for them to choose or limit the audiences of their communications, remove (or unlink from their profiles) information they feel is irrelevant or harmful, and otherwise make decisions about how to represent themselves.

There are, however, shortcomings. Social networks often have terms and conditions of service that allow them to unilaterally change their privacy settings over time, settings and controls vary across platforms, and default settings are often not the most privacy-protective, leaving vulnerable those who are less technologically-sophisticated.

The same problems exist with reputation management outside of social networks. Controlling search engine results, for example, requires the navigation of uncertain, ever-changing algorithms that differ between search engine providers. While there are a number of resources that teach search engine optimization (SEO) techniques, these methods are restricted to those who have the time and technical ability to employ them.

Market solutions: Reputation management

For those who can afford them, reputation management companies can play a leading role in managing one's information online. As described by Oravec, these are companies that "scout websites that post erroneous or damaging private information, correct or delete that info, or petition Web proprietors to take it down."[16] Many work to "bury" unwanted search results by creating and optimizing neutral or positive results.[17]

In the era of social media, however, when user-generated content is often what shapes reputation online, reputation management companies only go so far, offering short-term solutions for those who can pay.[18] As Oravec concludes, "Businesses such as KwickChex and Reputation.com can be of some assistance in reputational concerns, but more important will be lifelong awareness and vigilance on the part of individuals."

---

[13] Jurgenson, N., & Rey, P.J. 2013. The fan dance: How privacy thrives in an age of hyper-publicity. In G. Lovink & M. Rasch (Eds.), Unlike Us Reader: Social Media Monopolies and Their Alternatives. Amsterdam: Institute of Network Cultures.

[14] Mary Madden and Aaron Smith. May 2010. *Reputation Management and Social Media*. Pew Internet & American Life Project. http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx

[15] Kristen Purcell, Joanna Brenner and Lee Rainie, *Search Engine Use 2012*. March 2012. Pew Internet & American Life Project. http://pewinternet.org/Reports/2012/Search-Engine-Use-2012.aspx

[16] Oravec, J. 2012. *Deconstructing "Personal Privacy" in an Age of Social Media: Information Control and Reputation Management Dimensions*. In "International Journal of the Academic Business World" Volume 6 Issue 1.

[17] Ibid.

[18] Rosen, Jeffrey. July 2010. *The Web Means the End of Forgetting.* New York Times. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

Obscurity

We often hear the term "practical obscurity" used to describe information available publicly, but not expected to be found easily, in the offline world. "Practical obscurity has roots in geographic or physical boundaries that impede the understanding or discovery of information", write Hartzog and Stutzman, but that is not to say that there are no other ways to create obscurity. Information can be made obscure online—where the concept of physical distance doesn't apply—when information "lacks one or more key factors that are essential to discovery or comprehension." Those factors are (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity.[19]

Boyd and Marwick add to those factors in describing properties of networked sociality: in addition to the visibility ("scalability", as they call it) and searchability of information, they describe the automatic recording and archiving of online expression ("persistence") and the replicability of content.[20]

Those who use social media or otherwise share information online rely on norms and architecture and, to a lesser extent, market solutions to create and remove obscurity as desired.

Privacy settings, for example, can be used to address scalability, searchability, and identification; "whitewalling", or regularly deleting the information that one posts, prevents persistence,[21] as long as others are trusted to obey norms that prevent non-consensual replication; and "social stenography", in which users exclude unintended audiences through, for example, inside jokes or references, reduces clarity.[22]

Later we will discuss how obscurity could find a place in policy or law—and how it could apply in a right to be forgotten—as well as how public education about obscurity tactics could prove useful.

Vulnerable groups

Any policy relating to online reputation should seriously consider outcomes for vulnerable, stigmatized, and marginalized groups of people seeking to participate online.

In writing about students fearful of participating in online discussions, for fear of future reputational harm, Oravec warns that "timidity about intellectual interaction could inhibit exploration of important political and social concerns" and "result in a chilling effect".[23] When that chill affects those with radically less power—be it power through wealth, social standing, age, physical ability, or anything

[19] Woodrow Hartzog and Frederic Stutzman. 2013. *The Case for Online Obscurity*, 101 Cal. L. Rev. 1. Available at: http://scholarship.law.berkeley.edu/californialawreview/vol101/iss1/1

[20] Marwick, Alice, and danah boyd. 2011. *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*

[21] danah boyd paraphrased by Nathan Jurgenson and PJ Rey in *The Fan Dance: How Privacy Thrives in an Age of HyperPublicity*. 2013.

[22] Ibid.

[23] Oravec, J. 2012. Deconstructing "Personal Privacy" in an Age of Social Media: Information Control and Reputation Management Dimensions. In *International Journal of the Academic Business World* Volume 6 Issue 1

else—it takes on political significance. And as Elfreda Chatman found in her investigation of information poverty, being an "outsider" "necessitates heightened self-protective behaviour."

As more of life—be it social, professional, or democratic—is digitally-mediated, the unfettered ability to participate online is crucial for vulnerable groups. The recommendations in the following sections bear this in mind, but do not address it fully. It is strongly recommend that the OPC make a special effort to reach out to organizations that work with vulnerable individuals and marginalized communities—and when appropriate, to those individuals and communities themselves—in order to get a fuller picture of how and why they participate online, what their specific needs are, and how they feel they should be protected.

Taking action

This submission will not make specific recommendations to ameliorate the mentioned protections, but will point to a number of considerations that should be taken into account when implementing the following kinds of solutions.

Public education

Lawrence Lessig quotes Thurgood Marshall in describing the role of education: "Education is not the teaching of the three R's. Education is the teaching of the overall citizenship, to learn to live together with fellow citizens, and above all to learn to obey the law."[24]

Public education that takes rights-based approach to online reputation can help reinforce norms that protect online reputation, in addition to spreading knowledge of the law, how to make use of architecture-based controls, and how to evaluate protections offered across a multitude of platforms.

Education initiatives can also seek to introduce or name norms, such as a "share-alike" principle for obscurity. The term 'share-alike' is used by the Creative Commons project to name the requirement that copies or adaptations of a work be released under the same license as the original.[25] Hartzog and Stutzman adapt the term to apply to online obscurity, suggesting that "Internet users who were bound to a 'duty to maintain obscurity' would be allowed to further disclose information, so long as they kept the information as generally obscure as they received it." Defining and promoting obscurity measures—among other principles relating to online reputational control—could make it easier to communicate and reinforce existing norms around information sharing that protect the interests of individuals online.

[24] Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace.* p.129
[25] See https://creativecommons.org/licenses/by-sa/2.5/ca/ or https://wiki.creativecommons.org/wiki/Share_Alike

Architecture

As mentioned earlier, the availability of privacy controls appears to encourage Internet use, and social media sharing in particular.[26] It follows, then, that companies in the business of attracting people who generate content are well-served by making understandable privacy controls available.

As Oravec writes, "The fostering of a 'privacy/reputation divide,' in which some individuals are harmed because of their lack of time, resources, or technological ability, would have serious repercussions for organizations in the near future as individuals avoid or sabotage various social media venues."

Social networks could give individuals greater control of their online reputations by agreeing to standards for privacy controls that go beyond minimum requirements—so that those controls are stronger, vary less across platforms, and are more easily comparable and understandable to the average user—and agreeing to refrain from making their settings less privacy protective without users' explicit consent.

As well, default settings are powerful, and by starting new users—of social networks, websites, or even browsers—with very privacy-protective settings from which they could opt-out, architects of information-sharing platforms could encourage privacy protection, and give individuals a better sense of the privacy protections they may choose to give up.

Legal solutions

Legal solutions should be considered carefully, as the law draws a very specific line in the sand, and can be much more difficult to change than settings on a social media site.

When considering legal solutions, it is best to aim to only legislate against unwanted behaviour, not things that can lead to it or that allow for it. It is extremely important to avoid overreaching and potentially criminalizing legitimate free expression, or creating a chilling effect on Internet users.

In the case of online reputation impeding employment, for instance, what we really want to prevent are discriminatory employment practices. Human rights law and employment standards laws should be considered as possible vehicles for protecting disadvantaged groups and individuals who suffer as a result of damage to their online reputation. Perhaps improvement to these laws should be considered before seeking to introduce altogether new legislation. [27]

New laws may also be useful—Paul Ohm, a law professor at the University of Colorado, has suggested making it illegal "for employers to fire or refuse to hire anyone on the basis of legal off-duty conduct

---

[26] Jurgenson, N., & Rey, P.J. 2013. The fan dance: How privacy thrives in an age of hyper-publicity. In G. Lovink & M. Rasch (Eds.), Unlike Us Reader: Social Media Monopolies and Their Alternatives. Amsterdam: Institute of Network Cultures.

[27] In a study for the Canadian Centre for Policy Alternatives, Gwen Brodsky and Shelagh Day point to a number of flaws in BC's human rights system that stem from a lack of a Human Rights Commission. They point to the province's need for more human rights education, research, up-to-date guidelines and policies, and proactive inquiries, as well as a stronger and clearer complaints process.
https://www.policyalternatives.ca/publications/reports/strengthening-human-rights

revealed in Facebook postings or Google profiles"[28]—but should be considered carefully, and in consultation with citizens, employers, privacy experts, and free expression advocates.

Obscurity and the law

Hartzog and Stutzman raise the idea of using online obscurity as a legal tool. They suggest that obscurity could either be "conferred as a benefit or provided as a middle ground between total secrecy and complete public disclosure. This is particularly true for information that might be embarrassing but not damaging enough to warrant the full force of robust privacy and confidentiality protections. In this way, obscurity could be a less effective, but also less costly, remedy than complete confidentiality, anonymity, or the 'right to be forgotten.'"[29]

They also suggest online obscurity could be used as "a continuum to determine whether information is eligible for privacy protections", as a procedural protection, or be used in a "duty to maintain obscurity".

A right to be forgotten

In the European Union, the "right to be forgotten" exists at the intersection of data protection and intermediary liability.

The right of "protection of personal data" is enshrined in the *EU Charter of Fundamental Rights* separately from the right to "respect for private and family life". The *Charter* defines the former right as follows:

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

As Daphne Keller, Director of Intermediary Liability at the Stanford Center for Internet and Society, points out, data protection in the EU is "a broad right to limit processing of all information relating to oneself, not just information that invades personal privacy. Where it conflicts with other fundamental rights, including rights to receive and impart information, the rights at issue must be balanced."

If a Canadian right to be forgotten is to be considered to advance this personal data protection, we recommend that the OPC and other policy and law makers exercise great caution in assigning responsibility for it.

---

[28] Rosen, Jeffrey. July 2010. *The Web Means the End of Forgetting.* New York Times. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.I should note that Ohm's suggestion may be overbroad—after all, it is not illegal to publicly embarrass one's employer, but perhaps repeatedly doing so would be sufficient grounds for termination—and difficult to enforce. I raise it here only as an example, not as a recommendation.

[29] Woodrow Hartzog and Frederic Stutzman, The Case for Online Obscurity, 101 Cal. L. Rev. 1 (2013). Available at: http://scholarship.law.berkeley.edu/californialawreview/vol101/iss1/1

The EU's reliance on intermediaries—Google, in particular—to interpret and enforce their right to be forgotten has been met with a great deal of criticism from the technology sector and free expression advocates, among others.

Concerns with reliance on intermediaries

There are a number of concerns with reliance on intermediaries, but the ones that we find most notable are (1) that the interests of private companies do not necessarily align with the public interest, (2) that putting the onus on search companies and other intermediaries could be harmful to the digital economy, and (3) that companies are often risk-averse, and may err towards censorship to protect themselves.

Private companies will act to protect their own bottom lines. While this does at times align with the public interest—providing services for which there is a demand, for example—this is not the same as specifically working for the public. The actions of corporations are based on their own best interests, which will sometimes differ from what is in the public interest. It would be more appropriate to have a public body—with a public interest mandate, and accountability to the public—make decisions about how regulations should be implemented, and be responsible for actions taken. It seems wholly unreasonable to us that, under EU regulations, it is a corporation that is tasked with determining, case-by-case, how to "balance the privacy rights of the individual with the public's interest to know and the right to distribute information."[30]

Further, there are significant financial costs for carrying out this responsibility. The costs of implementing systems for members of the public to request that their information be obscured or removed, of employing professionals to make these decisions, and of insuring themselves against any fines for potential mistakes will have to come from somewhere. These additional costs could prevent smaller companies and new market entrants from being able to operate or compete effectively, or could translate to additional costs for consumers.

Finally, as we have seen in other jurisdictions, intermediaries have a documented tendency to "avoid risk and transaction costs by simply removing any challenged content."[31] As Daphne Keller explains, "Putting removal decisions in the hands of technology companies – as opposed to, say, content creators or national courts – is a recipe for over-removal of lawful expression." Keller cites reviews of removals

[30] "When you make such a request, we will balance the privacy rights of the individual with the public's interest to know and the right to distribute information. When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there's a public interest in the information — for example, we may decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials."
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en

[31] Keller, Daphne. October 2015. *Intermediary liability and user content under Europe's new data protection law*. http://cyberlaw.stanford.edu/blog/2015/10/intermediary-liability-and-user-content-under-europe%E2%80%99s-new-data-protection-law

under the *Digital Millennium Copyright Act* in the US[32], and studies of the actions of Dutch,[33] UK[34], and Indian[35] intermediaries as examples.

Other concerns

In addition to issues relating to intermediary liability, we want to highlight a number of other concerns with a right to be forgotten.

For one thing, a system that requires content be taken down or obscured from certain major websites, search engines, or social media platforms while ignoring others will exacerbate existing differences between those who know where to look for certain information and those who do not.[36] And as the Electronic Frontier Foundation's Danny O'Brien warns, "Popular search engines will list the best of everyone, and be compelled to disappear other facts. Meanwhile, a new market is created for mining and organizing accurate public data out of the reach of … authorities."

Another consideration is that allowing different websites to set up different processes for requesting or disputing a takedown may create confusion for users, and deter less technologically-literate people from using the system at all.

As well, it is important to insure against erroneous or malicious requests to delete online content. While data shows that 95% of Google privacy requests are from citizens, rather than criminals, politicians, or public figures,[37] it is vital that any request be considered carefully to avoid the deletion of information that is in the public interest.

Finally, we wish to highlight that jurisdictional issues may come into play. A Canadian body may not have the power to enforce its rules—such as in the Globe24h case, in which a Romanian website was ordered to take down information, but refused and faced no consequences[38]—or where a Canadian may want to hide information from parties living in another country. Technological solutions such as geoblocking may be available in the former case, but the latter case would require global cooperation. And, as Radsch remarks in her chapter, *Laws, Norms and Block Bots: A Multifaceted Approach to Combatting Online Abuse*, "in many parts of the world, including countries that do already have special mechanisms to

---

[32] See Jennifer Urban and Laura Quilter's 2006 review of DMCA removals and Daniel Seng's more recent work in the same area.

[33] Leyden, John. October 2004. *How to kill a website with one email: Exploiting the European E-commerce Directive* http://www.theregister.co.uk/2004/10/14/isp_takedown_study/

[34] Ahlert, C. et al. 2004. *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation* http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf

[35] *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*. 2011. http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf

[36] Bertoni, Eduardo. September 2014. The Right to Be Forgotten: An Insult to Latin American History. http://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be-forgotten_b_5870664.html?utm_hp_ref=tw

[37] Tippmann, Sylvia and Julia Powles. July 2015. *Google accidentally reveals data on 'right to be forgotten' requests.* http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests

[38] OPC "*PIPEDA Report of Findings #2015-002*" https://www.priv.gc.ca/cf-dc/2015/2015_002_0605_e.asp

address online abuse, law enforcement agencies are not equipped to deal with these complaints, and can even perpetuate the harm by requiring that offending content be further circulated."[39]

General recommendations

FIPA recommends that any measures taken to address online reputation concerns be handled by an appropriately-resourced body that is accountable to the public. The actions and decisions of this body should be the subject of robust oversight, including audits designed to ensure obscurity measures and takedowns are used appropriately.

When someone wishes to have information about them removed or obscured, the process should be relatively simple and standardized across platforms, and the evaluation criteria should be clear.[40] Whenever possible, the content creators or hosts should be notified and given the opportunity to dispute any removal or obscurity requests based on their own rights and interests or a public interest, and sufficient time should be taken to consider the legitimacy of the requests.

If it is decided that lawful content can be removed or obscured to protect reputational interests, public education efforts should be made so that Internet users know that information may be omitted from their searches or browsing. As privacy lawyer David Fraser has noted, "A search is 'tell me what is out there about X' and an omission without notice is a lie."[41]

Finally, further data should be collected about online reputation's effects on the online and offline lives of individuals. Any new policy or law that introduces takedown or obscurity requests should be accompanied by transparency reports with statistics on the number and nature of those requests, and should be subject to regular review.

Conclusion

The BC Freedom of Information and Privacy Association thanks the Office of the Privacy Commissioner of Canada for this opportunity to provide our views on this important issue.

In sum, we ask that the OPC consider the range of solutions to online reputation concerns outlined in this submission, and work to ensure that any position adopted includes strong considerations of the rights of content creators and hosts, and the public interest in information about legal and democratic practices and people in positions of power.

---

[39] From *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists* http://www.osce.org/fom/220411?download=true

[40] This was suggested by the Electronic Frontier Foundation and Article 19, in their Comments on the Intermediary Liability Implications of the EU General Data Protection Regulation (GDPR) https://www.eff.org/files/2015/11/20/comment_on_gdpr_final.pdf

[41] Fraser, David. October 2014. *Presentation: Right to be forgotten in Canada? Not so fast ...* http://blog.privacylawyer.ca/2014/10/presentation-right-to-be-forgotten-in.html

Canadians should be empowered to control their own reputations, and "selectively reveal [themselves] to the world."[42] We should be encouraged to participate online—in the digital economy, in online communities, in debates, in arts and culture, and whatever other opportunities are available—and know that we can do so without compromising our future, or the futures of our friends and loved ones.

We should also be held accountable for our actions. Our news and histories should be accurate. Our expression should not be limited unnecessarily.

It will take a great deal of consideration, and perhaps a few attempts, to strike the right balance. But with a rights-based approach and a willingness to listen and learn, it is entirely possible.

***

[42] Hughes, Eric. 1993. *A Cypherpunk's Manifesto*. http://www.activism.net/cypherpunk/manifesto.html