Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Meeting of Two Worlds: the Legal and Information Technology (IT) Universes

Online Identity: Between Privacy and Virtual Profiles

Jennifer Stoddart
Privacy Commissioner of Canada

February 2008

Table of Contents

Introduction

The vast expansion of online social networking sites such as Facebook and MySpace has introduced large numbers of people to the concept of a virtual profile. In many cases, the creation of an online profile is the first step (and a pre-condition) towards active membership in an online social network. Although a certain amount of personal information is generally required in order to join such services (such as a valid email address), there is usually considerable individual choice involved in the creation of one's virtual profile: the choice to join a particular service, what information to provide or withhold, and the language used in providing that information. To some extent, the virtual profile is a vehicle of creative self-expression, allowing an individual to tailor his profile in order to reflect the specific ways in which he would like to present himself online. Members of online social networking services are arguably learning about how the manage their identity online. Or are they?

While many Canadians may not choose to join a social networking site and create an intentional virtual profile, they might be surprised to learn that they likely nevertheless possess an unintentional or passive virtual profile, which may correspond poorly to the kind of profile they would create themselves. Frequently, the "intentional" profile that is carefully crafted on a social networking site is only the tip of the iceberg in terms of one's online identity. Few people have a clear sense of just how much information about them makes its way online or of the ways in which such information can contribute to their virtual identity. Even more surprising is the extent to which this unintentional virtual profile can impact an individual's non-virtual or offline existence. This paper examines the potential scope of a virtual profile, identifies some of the privacy concerns raised by such profiles and offers suggestions for developing our capacity to control our identity online --- and therefore offline.

Virtual profiles: a preliminary overview

Intentional/active profile

An online intentional profile can take many forms. The social networking site profile is in some ways simply a personal take on the kind of biographical information provided by individuals for professional reasons, such as faculty members at a university or lawyers at a law firm. In all cases, the information is carefully selected and presented with a particular audience in mind; in the case of the social networking tool, the profile creator may also have some control over the audience that will access the finished profile. The defining element of an intentional profile is the creator's control over its contents and presentation.

Unintentional/passive profile

An individual’s unintentional virtual profile is the complete trail of personal information about that individual which can be found online. The sources of such information may be disparate and in many cases, the information may have found its way online without the involvement of the individual concerned. The possible range of such information is limitless: a name added to a petition; contact information obtained through online directory services; a comment posted on somebody’s blog; a name appearing on a list of donors to a particular cause; a caption under a photo taken at a high school reunion.

Profile elements can be unintentional for many reasons. It may be that the information was not obtained from the individuals concerned and that they were not consulted before it was posted online. Information that was collected offline could also get posted online without the individual knowing that it was destined for unrestricted online dissemination. Information originally intentionally posted online might be considered part of the unintentional profile based on the length of time it remained available online. Thanks to cached pages, even information that has been deleted by the poster can persist online and be retrieved by means of online search tools long after deletion has supposedly taken place.

The unintentional virtual profile is therefore a combination of all of these different kinds of personal information as encountered online. An idea of the range of information available can be gained by performing a simple search of an individual’s name using any of the major search engines. The result is likely to be a broad range of information, presented without concern for currency, accuracy or context. Taken on an individual basis, many such ‘hits’ might appear innocuous. When taken cumulatively however, the unintentional profile emerges, with or without the assistance, knowledge or consent of the affected individual.

There is however one additional layer to a passive profile. Thanks to various kinds of tracking devices, an individual’s online activity leaves a trail which is potentially of great interest to others. Although individuals are least likely to ever see this layer of their virtual profile in concrete fashion, there is every likelihood that it is ‘fed’ back to them by means of marketing targeted specifically to choices they have made in their online activity such as websites visited and searches performed.

Potential audiences for profile information

While the average individual is unlikely to have a good grasp of what their complete virtual profile looks like, there are potential audiences who make it their business to do so. An awareness of the range of potential audiences and of the reasons behind their interest in what might otherwise seem like innocuous personal information may assist individuals in exercising control over their online identities.

Data brokers

Given the tremendous wealth of information that is available online, it is not surprising that organizations now exist which are in the business of gathering and selling personal information. The largest of these data brokers hold collections of documents in the billions. This kind of ‘piggy-backing’ on otherwise available personal information raises interesting questions about the notion of what constitutes “publicly available” information. It also raises concerns about the adherence to the principle of purpose-based consent, since such gathering and subsequent disclosure will in most cases be well beyond the collection, use or disclosure originally contemplated by the affected individual.

Marketing

As mentioned above, many elements of one’s online profile are of interest from a marketing perspective. Indeed, it is the perceived value of such information which sustains many supposedly ‘free’ online services and activities, such as social networking sites, web-based email and search engines. While advertisers have long had an interest in this kind of profile information in aggregate form, the more sophisticated evolution of the use of this information is targeted marketing. An individual’s interests, tastes, likes and dislikes, as reflected both by the information about them that has been posted on the Internet and by the choices they make while online, is reflected back to them in advertising designed to be all the more effective because it has been tailored, either to a particular demographic or at times to that particular individual.

Identity theft

There is also a considerable amount of criminal activity centred around the unauthorized collection, use and disclosure of personal information online. An individual’s virtual profile may provide sufficient information to allow an identity thief to impersonate that individual for the purpose of engaging in fraudulent activities. Where the accessible virtual profile is inadequate for this purpose, identity thieves may supplement the profile by other means, whether by testing the safeguards employed by those organizations which have custody over sensitive personal information (such as financial institutions) or by phishing for additional personal information directly from the individuals concerned.

Investigations and monitoring

The Internet is also an important resource for those engaged in investigative or surveillance-type work. While some may resort to use of a data broker in order to obtain the desired information, in many cases, the use of a search engine will suffice. At the simplest end, many employers now perform an Internet search of a candidate's name as part of the recruitment process. While a candidate may not be warned of such a search or told that it has taken place, for many employers, such searches have become common practice.

Seemingly innocuous personal information can also be put to more sophisticated use. By virtue of what is commonly referred to in intelligence circles as the "mosaic principle", pieces of information which appear insignificant on their own, can, when placed together, add up to something of value. While such compilation work is painstaking, the volume of information available on the Internet and the length of time for which it remains accessible both encourage perseverance in such efforts. It should also be noted that layering of data can take what would otherwise not constitute personal information (because it does not allow for the identification of a particular individual) and turn it into personal information when combined. For law enforcement authorities, the information available on the Internet provides a warrant-free means of engaging in important investigative activity.[1] And, while such work is undertaken by law enforcement authorities, they do not have a monopoly on such investigative activities. The private sector engages in similar activities, both where it has been deputized to do so by the public sector and in the context of more general private-sector investigative activity.

Virtual meets the real world: potential impacts

The discussion of audiences potentially interested in the information contained in a virtual profile makes it clear that one's virtual identity can have important real-life impacts.

The Canadian military recently issued a warning to its members and their families regarding the posting of personal information online, particularly on social networking sites, reminding them that what seems harmless and insignificant to the person posting the information could become considerably more dangerous in other hands if placed alongside other pieces of information by someone willing to patiently piece things together.[2]

In another setting, employees had a rude awakening when information they had posted on Facebook was disclosed to their employer by former colleagues. The

[1] The use of the Internet as an investigative tool (and in some cases an alternative to the obtention of a warrant) has important implications for the privacy rights guaranteed under section 8 of the Charter.

[2] "Military warns soldiers not to post info on Facebook", CBC News, February 25, 2008, www.cbc.ca.

employees had posted questionable information directly related to their jobs online, including photographs of the employees in uniform which were taken in direct violation of their employee code of conduct. As the employer, the Canada Border Services Agency indicated in an internal memorandum, "Even off-duty conduct becomes a work-related matter if it jeopardizes the agency's reputation or programs."[3] While in this case the behaviour appears to have been clearly inappropriate and the individuals who posted the information appear to have chosen to link their behaviour to their place of employment and to take little in the way of precautions to limit access to their posts, one can easily imagine scenarios in which the facts were less heavily weighted in favour of the employer.

Much online activity takes place with little regard to national borders and the collection, use and disclosure of data online may in fact involve several jurisdictions. In a recent case, the Executive Director of the Canadian Internet Policy and Public Interest Clinic contacted a U.S.-based online data broker and requested a profile of herself. When the profile arrived, it turned out to be a largely fictitious compilation. Not only was this inaccurate profile available to anyone who requested it for a fee, the individual profiled would not necessarily ever learn that such a profile existed or had been obtained by other people.[4]

Privacy Concerns

Online identity raises significant privacy concerns. The fact that a virtual profile continues to develop even without conscious input on the part of the affected individual suggests the average person lacks control over his or her online identity. The result is a substantial reduction of the private sphere and a direct challenge to an individual's reasonable expectation of privacy. Since it is possible to develop a virtual profile without ever going online, it is difficult to conceive of opting-out of this process. Furthermore, the elements that add up to constitute one's online profile include many of the basic transactions and interactions which are essential to our membership in modern society, such as banking, bill payments or registration for government services. To some extent, we cannot avoid leaving an identity trail, both offline and online. The growing importance of online identity in our lives also means that we cannot be taken to waive fundamental privacy rights for the online portion of our existence.

Managing Online Identity

Although the task of managing one's online identity may appear daunting, there are nevertheless simple steps that individuals can take to protect their privacy online and in doing so, to manage their online identity. At a minimum, we can be masters of our intentional profiles. By becoming aware of the potential attractiveness to others of the information we post about ourselves online, we

[3] "Student recruits unfit for service, say former border guards", CBC News, October 1, 2007, www.cbc.ca.
[4] *Lawson v. Accusearch Inc*., [2007] 4 F.C.R. 314 (F.C.).

can make more informed choices about the identity trail we choose to create. For example, we know that certain key pieces of personal information provide the foundation for identity theft and should not be disclosed other than in a secure context (for example, Social Insurance Numbers, date of birth, address and phone number). We can also make it a practice to learn about the possible future dissemination of information before we provide it. For example, if information will not be protected and will be available to web-based search engines, we can at least be aware that cached versions of that information will be available as search results long after the information has been removed from the site where it was posted.

It is also worth remaining aware of the purposes behind the collection of personal information online. In the case of the social networking sites for example, it may appear to the individual users that the purpose of the collection of their personal information is in order to allow them to fully participate in the resulting social network. While this purpose may be valid, it is not the only purpose behind collection and may indeed be secondary to the purpose of collection for marketing reasons. Many online services offered at no apparent cost to the user are in fact commercially supported by the value of the personal information the individual provides as a condition or result of using the service. As with offline loyalty programs, by understanding what actually makes a particular service viable from a commercial perspective, we will be better equipped to weigh the pros and cons of becoming participants and, in the case of many online activities, to make informed decisions about the extent of our participation.

OPC Initiatives

The OPC has engaged in a number of public education activities designed to raise awareness of the need to protect personal information online, including in particular online environments such as social networking sites. Although there has been tremendous expansion beyond youth in terms of the demographic making use of social networking sites, the OPC is conscious of the fact that the use of such services among young Canadians is ubiquitous. Young people need specific tools in order to help them make informed choices about online identity, and those tools need to reach out to young people in ways that are meaningful. With this in mind, the OPC has created a short video, entitled “What does a friend of a friend of a friend need to know about you?” on the privacy implications of social networking sites. The video, which is available on both our website and on our YouTube channel, has been viewed over 5000 times on YouTube.

We have also prepared a number of tools to help people protect themselves from identity theft. “A Primer on Identity Theft” as well as an “Identity Theft Checklist” are just two examples of the tools available on our website. An individual can greatly enhance his or her protection against identity theft by taking a few simple

steps; our goal is to make people aware of a range of practical changes that can easily be implemented.
The privacy issues related to our online lives evolve in tandem with the technology that facilitates online activity and with our uses of that technology. The OPC must anticipate these developments in order to be well-positioned to keep the public informed of the privacy implications of our online existences and to provide suggested responses to those implications. As part of this commitment, the OPC funds a Contributions Program of independent research in areas of priority identified by the OPC on an annual basis. Past research has included ground-breaking work in the area of online identity as well as a comprehensive review of the data brokerage industry in Canada.

Conclusion

The social transformation that has taken place in the span on a single generation due to the Internet is nothing short of staggering. Our online activities are increasing in quantity and diversifying in scope in ways unimaginable only a decade ago. This change has tremendous potential benefits in terms of fostering community, enhancing communication and promoting creativity. The aim of increased privacy awareness is not to discourage us from embracing the full potential of the Internet. What matters is that we each acquire the tools necessary to navigate these new virtual worlds in ways that allow us to actively benefit from the potential of online activity while maintaining a sense of control over its impact on our lives, both online and offline.

The Privacy Commissioner of Canada, Jennifer Stoddart, would like to express her gratitude to Kate Wilson, Legal Counsel in the Office of the Privacy Commissioner of Canada, for her indispensable assistance in the preparation of this paper.