How To Get Your Personal Information From Social Networking Companies

January 26, 2013 :: Version 1.1

Contents

About the CATSMI Project

The Canadian Access to Social Media Information (CATSMI) Project operates out of the University of Victoria. It is a distinctly Canadian research project, but we believe that our findings have a very wide relevance. The central hypothesis of this project is that the evolution of a more "social web" poses significant challenges to theories of informational privacy as well as to the national legal systems and regulatory policies that have been based on these theories.

The main objective of the Project is to determine how the expectations of social networking websites and environments, whose raison d'etre is the facilitation of the sharing of personal information about and by users, can be reconciled with prevailing understandings about "reasonable expectations of privacy" and the existing regimes that are designed to protect personal data. Organizations have to make decisions about the granularity and range of privacy choices to offer users. Are there significant variances between organizations' perspectives and policies on access to personal information by data subjects on the one hand, and those of government authorities on the other? Are data subjects meaningfully made aware of their own rights to access data, and the capabilities of authorities to access the same subjects' data?

The Project has adopted a three-track process to understand the relationship between social networking services and government intelligence and policing services. **First**, we have analyzed the stated policies and publicly available lawful access documents that social networking services have prepared. These documents were accessed via public Internet repositories or, in one case, through private sources. They have revealed how personal information is made available by social networking services, and the conditions for providing it to government agencies.

Second, researchers investigated whether members of social networking services could access their own records and correct misleading or incorrect fields, and thus enforce their privacy rights under the Personal Information Protection and Electronic Documents Act (PIPEDA), and substantially similar provincial legislation. This approach allows us to ascertain the actual access that Canadians might have to the profiles that they, and networking services they are associated with, are developing. It also let us ascertain whether records provided to service members contain similar, more, or less information than the data fields that may be made available to law enforcement.

Third, Project members have evaluated how existing disclosure policies are, or would be, affected by forthcoming Canadian lawful access legislation. This final level of analysis will clarify whether Canadian authorities will have new powers in excess of social networking companies' existing disclosure conditions.

The outcome of our analysis is a better understanding of how Canadians' information is collected and made available to social network members and third-parties. By analyzing the practices of major social networking sites we have sought to make it clear to Canadians how their personal information might be accessed by authorities.

CATSMI's research is funded through the Office of the Privacy Commissioner of Canada's Contributions program. The use of these funds is independent of the Commissioner; as such, information in this document reflects work that emerges from independent academic research and does not necessarily reflect the Privacy Commissioner's own position(s). Funding has also come from a Social Sciences and Human Research Council (SSHRC) grant: "Social Networking and Privacy Protection: The Conflicts, the Politics, the Technologies (2010-13).

Introduction

Canadian news routinely highlights the 'dangers' that can be associated with social networking companies collecting and storing information about Canadian citizens. Stories and articles regularly discuss how hackers can misuse your personal information, how companies store 'everything' about you, and how collected data is disclosed to unscrupulous third parties. While many of these stories are accurate, insofar as they cover specific instances of harm towards subscribers, they tend to lack an important next step; they rarely explain how Canadians can become educated on the data collection, retention, and disclosure processes of social networking companies.

Let's be honest: any next step has to be reasonable. Expecting Canadians to flee social media en masse and return to letter writing isn't an acceptable (or, really, an appropriate) response. Similarly, saying "tighten your privacy controls" or "be careful what you post" are of modest value, at best. Today, many Canadians are realizing that tightening their privacy controls does little when the companies can (and do) change their privacy settings without any notice. This information in this document is inspired by a different next step. Rather than being inspired by fear emergent from 'the sky is falling' news stories, what if you were inspired by knowledge that you, yourself, gained? In what follows we walk you through how to compel social networking companies to disclose what information they have about you. In the process of filing these requests you'll learn a lot more about being a member of these social networking services and, based on what you learn, can decide whether you want to change your involvement with particular social media companies.

We start by explaining why Canadians have a legal right to compel companies to disclose and make available the information that they retain about Canadian citizens. We then provide a template letter that you can send to social networking organizations with which you have a preexisting relationship. This template is, in effect, a tool that you can use to compel companies to disclose your personal information. After providing the template we explain the significance of some of the items contained in it. Next, we outline some of the difficulties or challenges you might have in requesting your personal information and a few ways to counteract those problems. Finally, we explain how you can complain if a company does not meet its legal obligation to provide you with a copy of your personal information. By the end of this post, you'll have everything you need to request your personal information from the social networking services to which you subscribe.

Cite As

Christopher Parsons. (2013). "How To Get Your Personal Information From Social Networks," *The CATSMI Project*. Published January 26, 2013. Available at: http://catsmi.ca/resources/public-resources.

Why Can You Request Access?

Per Canadian privacy law, all Canadians can request that companies explain and disclose the kinds of personal information that they retain about the requesting Canadian citizen. Section 4.9, Schedule 1 of Canada's federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), legitimizes such requests and compels organizations to respond to requests when those companies have significant connections with Canada. The Privacy Commissioner of Canada's website, when discussing cloud-computing based services (e.g. social networking services like Facebook and Twitter), reads, "Where the Privacy Commissioner has jurisdiction over the subject matter of the complaint but the complaint deals with cloud computing infrastructure and thus is not obviously located in Canada, current jurisprudence is clear that the Privacy Commissioner may exert jurisdiction when assessment indicates that a real and substantial connection to Canada exists." Engaging in commercial relationships with Canadians can be said to constitute such a connection.

Moreover, the question of whether the Commissioner has jurisdiction over foreign companies has been settled in Canadian case law. Major social networking services establish an economic, and thus significant, relationship with Canada by providing services to Canadians. Consequently, Canadians can avail themselves of PIPEDA to compel companies to disclose what information they have collected and retained about Canadian citizens, which includes everything from photos during summer trips, to private conversations with other subscribers using the social networking service, to phone numbers it has stored, to the metadata (e.g. GPS information) that the service has collected and stored.

A Template to Request Access

The following template can act as the first, though perhaps not final, component of your adventure to learn what personal information a social networking giant retains about you. The text is written with the assumption that you are using email to submit the request, though with minor modifications it could be used to file a request through other mediums; some services may force you to mail in a physical letter, and others might try and force you to use their own request tools. Feel free to modify the text of the template as you deem necessary. The template tells a company to disclose all of the information they retain about you, including information that is often hidden when you update your status page or post a photo. A brief discussion on the significance of some of the requested items is found after the template.

Subject: Access Request

[Your mailing address]

[Date]

[Mailing information for social networking company]

To: [Department of social networking company]

Re: [Your subscriber username]

Dear X:

I am subscriber to your service, and am interested in understanding the kinds of personal information that you maintain about me. Accordingly, this is a request to access my personal data under Section 4.9 Schedule 1 of Canada's federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA). [I also note that you have committed to providing this access to personal data in your privacy policy at: URL.]

I am requesting a copy of all records which contain my personal information from your organization. The following is a non-exclusive listing of all information that [name of organization] holds about me, including:

- All logs of IP addresses associated with my account (because these are bound to my password-authenticated account and are thus identifiable)
- Any records of contacts stored on mobile devices that may have been collected in the course of installing your organization's mobile app or client, or obtained through other contact upload systems
- Any records of disclosures of personal information to other parties, including law enforcement (such records of disclosures themselves constitute personal information)
- Metadata that is associated with communications content that I have made available to, or produced via, your organization's services (e.g. Geo-locational information, date content was created, biographical information embedded with content but hidden from visualized display of content, deletion statuses associated with content that remains in your database(s))
- Information that, while no longer visualized from the front-end interface presented to end-users (often regarded as 'deleted information'), remains in your backend databases

If your organization has other information in addition to these items, I formally request access to that as well.

You are obligated to provide copies at a free or minimal cost within thirty (30) days in receipt of this message. If you choose to deny this request, you must provide a valid reason for doing so under Canada's PIPEDA. Ignoring a written request is the same as refusing access. See the guide from the Office of the Privacy Commissioner at: http://www.priv.gc.ca/information/guide_e.asp#014. The Commissioner is an independent oversight body that handles privacy complaints from the public.

Please let me know if your organization requires additional information from me before proceeding with my request.

Here is information that may help you identify my records:

Full Name: [Name]
Account Number: [Number]
Handle: [Handle]
Email Associated With Account: [Email address]

Sincerely,
[Name]

Explaining the Template

It may not be self-evident why all the items in the template are important or what they mean; what is the significance of the requested data? By the end of this section, these kinds of questions will be covered, giving you a better idea of how and why certain types of data are relevant to your query.

- Name of department: if possible, you want to direct your request to the company's privacy office/officer. Alternately, if the company has an executive office email account you could send the message there. Failing either of those, try the general contact email address, or (if it's listed) print a copy of your request and physically mail it to the company.
- IP addresses: though IP addresses aren't perfect online identifiers, they are often persistently linked to specific routers. This is true even if you have a 'dynamic' broadband connection in Canada; quite often it can be weeks or months before a new IP address is assigned to any given router. In the case of businesses that have dedicated IP addresses it is possible to correlate (roughly!) the geographical regions you visit. Moreover, should the social networking company in question ever disclose the IP logs linked to your account to third-parties, those third-parties could figure out where you've physically been present (e.g. coffee shops, libraries, airports, or anywhere else with a wifi access point). Now, this kind of investigative work would require compelling the relevant ISPs linked with the IP address to reveal what modems were associated with what IP addresses, including when, and where, those routers are located. So while this isn't the easiest way to figure out where you've been, it's a tried-and-tested method that authorities, lawyers, and other third-parties around the world have used for years.
- Contact information: social networking companies rely on your contact books to find your friends on social networks that you've been a part of for a long time. On the one hand, this information could be used temporarily to see whether people you know are on the service, and after this action, the contact book information could be purged. Alternately, this information could be retained indefinitely. It's nice to know if, when you said "yes" to grant a company access to your contacts,

the company took that to mean they could store that information forever, or if they only used it for the temporary (and reasonable) purpose for which you provided the authorization in the first place.

- Data disclosure: though it's somewhat self-evident, you likely want to know if the social network in question has disclosed your information to another party. Given the prevalence of policing bodies' access to citizens' social networking information, it is revealing to discover that (a) the information was disclosed; (b) you were never contacted by authorities. While this could be evidence of an ongoing case against you, it might just as likely suggest that your data could end up as part of a fishing expedition and you just happened to get caught up in the net. Still, it's not just the police that you might be mindful of: has your data been sold to marketers? Political parties? Other identity brokers? Insurance companies? In essence, there are lots of groups that are interested in your data, but you'll likely only discover if they've received it by asking your social networking company about data disclosures.
- Metadata: Metadata is probably the part of your request that is most likely to appear Greek to you (assuming, of course, you don't speak Greek!). Metadata is also one of the most important categories of data that you want companies to reveal to you. In essence, what you're asking is this: how much information about you and your information is the company in question collecting? Does it capture browser fingerprints, which can identify your web browser with high degrees of accuracy? GPS information? Biometric data? Are there data records that are 'written' when you publish a comment that are invisible unless you dig below the surface? Quite often metadata will be used for internal or external analysis to discriminate against various 'types' of users, with the purposes and related discrimination manifesting a bit differently on each social network. If you get this kind of information you might contact your closest geek friend, who can help you decode whatever information you get back. Importantly, before you can ascertain what kind(s) of service discrimination are possible, and are perhaps occurring to you, you need to know all the data, and data about data, that the company is generating about you.
- Non-deleted deleted data: The final category refers to data that you have 'deleted' but that wasn't actually deleted from the company's servers. If you read through many of the privacy policies linked with major social networks you find that they rarely provide guarantees to delete your data, and that some go so far as to assert that they cannot, or will not, remove some of your data. In essence, some social networks will suppress data from public viewing while retaining that very same data for internal purposes. In filing your request, you might find that the network in question really just suppressed information that you'd thought had been permanently deleted.

If you're lucky in filing one of these requests you could get a whole lot of information from the company you send a letter to. Alternately, you could get next to, or absolutely, nothing from the company in question. Either way, it's not uncommon to encounter some stumbling blocks between you and the data that social networking companies retain. In

the next section I discuss some of the stumbling blocks between you and the data social networking companies hold, and a few tips to help you overcome those blocks.

Is It As Easy as Just Asking?

In the best of cases you'll deal with a company that has a privacy officer or department that is familiar with these kinds of requests. The same company, ideally, will already have policies in place to facilitate a smooth response to your request. Unfortunately you're likely to discover more companies ignore you, or actively resist disclosing information, than companies who happily work with you to disclose your personal information. So when you have to push to get your information, what can you do?

A Polite Reminder

Companies, like individuals, often forget about things. Bureaucracies are a mess, and things can get lost, especially when they're trying to deal with actions that they encounter less often (e.g. your access request) and will cost them money to fulfill. It's not unusual for smaller social networks to retain counsel to figure out what your request might really even mean! The first thing you can do is send a polite note or reminder a few days after your first request if you haven't heard anything back. Ideally this (re)initiates the company's internal policy wheels, and your data might be on its way soon thereafter. However, if thirty days go by and you don't hear anything back, send a polite note. If you still haven't heard from them a few days after this reminder then you can complain to the federal privacy commission (more on that below).

What If the Company Says "No"?

When you've been told "No" you can submit a follow-up letter that looks like the one below. You'll probably want to modify it a bit, depending on your correspondence with the company/representative in question. Note that in the original template, above, you didn't explain in depth that the company had a very clear legal obligation to provide you with your information. The template below, however, does lay out those requirements. I've assumed that you're corresponding through email, but if you have to communicate through other means only minor changes should be required.

Subject: Access Request

[Individual's mailing address]

[Date]

Re: [Social networking service user name]

Dear [X],

Thank you for your timely response.

In your email, dated [date], you state that [social networking company] will not provide information that was requested pursuant to Section 4.9 of Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") on the the following bases:

[Restate, in ordered number format, the reasons the company provided for not providing your information.]

[Social networking company]'s collection, use, and dissemination of my personal information for commercial purposes means that [social networking company]'s actions fall within the scope of PIPEDA. Canadian case law and the Office of the Privacy Commissioner of Canada have previously demonstrated that foreign companies have an obligation to comply with PIPEDA.

Specifically, the Commissioner's website, when discussing cloud-computing based services, reads, "Where the Privacy Commissioner has jurisdiction over the subject matter of the complaint but the complaint deals with cloud computing infrastructure and thus is not obviously located in Canada, current jurisprudence is clear that the Privacy Commissioner may exert jurisdiction when assessment indicates that a real and substantial connection to Canada exists" (Source: http://www.priv.gc.ca/information/pub/cc_201003_e.asp#toc5). Engaging in commercial relationships with Canadians can be said to constitute such a connection. Moreover, the question of whether the Office has jurisdiction over foreign companies has been settled in Canadian case law (See: http://www.priv.gc.ca/information/pub/cc_201003_e.asp#toc3c).

Given that [social networking company] is engaged in commercial operations in Canada, vis a vis providing its service to Canadians, it can be said to possess a real and substantial connection to Canada. As a result, it is subject to Section 4.9 of PIPEDA, Schedule 1. In light of this, I would firmly reiterate my request that [social networking company] disclose personal data that it has collected about me, as outlined in my letter to [social networking company] in my previous letter dated [Date]. For convenience sake, I have attached this letter to this email in a .pdf format.

Sincerely,
[Name]

In a situation where the company still refuses to provide you with your personal information you can file a complaint with federal privacy commissioner. Such a complaint will (hopefully!) provide access to your personal information.

Complain to the Privacy Commissioner of Canada

The federal Office of the Privacy Commissioner of Canada (OPC) is a designated ombudsperson; the office effectively acts as the federal point-institution for all things privacy. If a company either refuses to disclose your information, or is providing information in a manner that you think is misleading or false (e.g. they say they've given you everything, but you have very good reason to believe that the company has/is

collecting further information about you) then you have the option of complaining the OPC. In your written complaint you'll want to explain everything that you've done to date: when you sent your first request, responses from the company (if there have been any), and why you have a problem with their (lack of) response. Note that the OPC does not accept complaints by email, so you'll need to file by letter mail to the address below:

Office of the Privacy Commissioner of Canada
Place de Ville, Tower B
112 Kent Street, 3rd Floor
Ottawa, Ontario K1A 1H3
Telephone: 613-947-1698 or 1-800-282-1376
Fax: 613-947-6850

The OPC can act as a mediator between you and the social networking company, helping all parties involved to resolve the company's failure to disclose your information. Alternately, they can investigate the company's practices to see if they are actively contravening federal law. For the purpose of Canadian law, it doesn't matter if the company is located in the United States, China, or Germany, though for practical (read: lack of resources) reasons, the OPC may decline to pursue a full investigation. Ideally, however, getting the OPC involved will mean that the company will (eventually) disclose your personal information.

Conclusion

So, hopefully after submitting your request you'll receive a copy of the information that a company has collected about you. This should include information that you, yourself, have submitted to the company: all of your Tweets, messages, check-ins, and other content that you generated in your name while using the service. With a stack of information in front of you that has been provided by social networking services, you can think about whether the companies are collecting a lot of data about you, and whether you're comfortable with the companies collecting, retaining, and using that data.

To be clear, you might be entirely satisfied with the data being retained and collected. The usage of your data, with or without your knowledge, may not bother you either. But, without a doubt, you'll have a better idea of what kinds of information the company in question holds about you. Maybe you'll change your online habits, maybe you won't, but your decision will be firmly rooted in your own experiences instead of from TV, radio, and print stories that regularly warn you about the dangers of social media.

Now, before you rush off to file your access request(s), there is one last concern that might come to light: the company in question might steadfastly refuse to communicate with either you or even the federal Privacy Commissioner's office. The company might operate as an information black hole, where your personal information goes in and nothing (evident) comes out. If you encounter this kind of situation, while you won't know what the company is collecting, you'll at least be in a better position to evaluate

whether you want to remain a subscriber of that company's social network, or if you'd rather, take your personal information elsewhere.

About the Authors

This document was researched and written by Christopher Parsons.

Christopher Parsons is a privacy-by-design ambassador, a well-recognized member of the Canadian privacy community, and a Principal at BlockG Security and Privacy Consulting. He has over a decade's experience working with challenging privacy issues that are linked to digital technologies. He specializes in how Canadian privacy law intersects with digital systems, and the implications of such law on the development and deployment of novel projects and practices. Christopher is presently completing his Ph.D in the Department of Political Science at the University of Victoria, where he is a fellow at the Centre for Global Studies. He has published in the Canadian Journal of Law and Society, European Journal of Law and Technology, Canadian Privacy Law Review, CTheory, and has book chapters in a series of academic and popular books and reports.

Legal Information

Electronic version first published at www.catsmi.ca in Canada in 2013
by The Canadian Access to Social Media Information (CATSMI) Project.

Header designed by Karen Yen of Can Poeti Branding and Design.

Information presented in this document is for academic and educational purposes only. These materials do not constitute solicitation or provision of legal advice. The CATSMI Project makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Nothing herein should be used as a substitute for the legal advice of competent counsel.