Disclosing Information to Law Enforcement Authorities Privacy Policy and Terms of Service Analysis

March 18, 2013 :: Version 1.0

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. This has 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).

Overview of Law Enforcement Guide Handbook Analysis

Social networking companies such as Club Penguin, LiveJournal, and Nexopia note in their Terms of Service and Privacy Policy pages how, and under what conditions, the companies will disclose subscriber information to authorities. These Terms and Policies were accessed via companies' public websites. As part of the Canadian Access to Social Media Information (CATSMI) Project we consulted these documents to understand how different companies were willing to disclose this information.

The tables below present information taken from the companies' websites, where we have collected information about what these companies publicly tell subscribers about disclosing information to law enforcement. Given the relative sparseness of information on these companies' websites, we have refrained from a conducting a detailed evaluation of how corporate disclosures would, or would not, intersect with recently proposed Canadian lawful access legislation. While Law Enforcement Guide handbooks can run dozens of pages, the information expressed through these public Terms of Service and Privacy Policy documents tends to only run a few paragraphs, at most.

Importantly, the tables below only have detailed information when we lacked access to a company's lawful access disclosure handbook. These handbooks provide substantially more information concerning corporate disclosure practices. For our detailed evaluation of these handbooks we refer you to our "Law Enforcement Authorities Handbook Analysis" document, available at the CATSMI Project's website, www.catsmi.ca.

This document is current as of March 18, 2013. It is possible that between our collection of data and your accessing this document that policies may have changed

Cite As

Adam Molnar and Christopher Parsons. (2013). "Disclosing Information to Law Enforcement Authorities Privacy Policy and Terms of Service Analysis," *The CATSMI Project*. Published March 18, 2013. Available at: http://catsmi.ca/resources/public-resources.

Summaries of Disclosure Statements

Social Networking Company	Findings	Source	Date
Blogger (Google)	See Law Enforcement Handbook		
Club Penguin	"We may disclose information where we are required to do so by law, for example, in response to a court order or a subpoena, or where we disclose information to data processors who act on our behalf (service providers or other group companies who provide support for the operations of our website and who do not use or disclose the information for any other purpose). To the extent permitted by applicable law, we also may disclose PII in response to a law enforcement agency's or other public agency's (including schools or children services) request or if we feel that such disclosure may prevent the instigation of a crime, facilitate an investigation related to public safety or protect the safety of a child using our website, protect the security or integrity of our website, or enable us to take precautions against liability."	Privacy Policy	Jan 11, 2011
Facebook	See Law Enforcement Handbook		
Flickr (Yahoo)	See Law Enforcement Handbook		
Foursquare	"Sharing with Partners, in connection with business transfers, and for the protection of Foursquare and others: Protection of Foursquare and Others: We may release Personal Information when we believe in good faith that release is necessary to comply with the	Privacy Policy	Jan 28, 2013

	law, including laws outside your country of residence; enforce or apply our conditions of use and other agreements; or protect the rights, property, or safety of Foursquare, our employees, our users, or others. This includes exchanging information with other companies and organizations (including outside of your country of residence) for fraud protection and credit risk reduction. International Users If you are located outside of the United States, please note that this site is hosted on our computer servers in the United States. Therefore, your information may be processed and stored in the United States. As a result, United States federal and state governments, courts, or law enforcement or regulatory agencies may be able to obtain disclosure of your information through laws applicable in the United States. Your use of this site or the Service or your submission of any Personal Information to us will constitute your consent to the transfer of your Personal Information outside of your home country, including the United States, which may provide for different data protection rules than in your country."		
Google +	See Law Enforcement Handbook		
Instagram	See Law Enforcement Handbook		
LinkedIn	See Law Enforcement Handbook		
LiveJournal	"Safety and Security: We may share your personal information with U.S. Law enforcement officers to investigate, prevent, or take action to prevent or stop	Privacy URL	Dec 12, 2010

	illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of LiveJournal's TOS, and/or if it is necessary to comply with, and/or cure a potential violation or breach of, U.S. law."		
Meetup	"3.3. Required disclosures. Though we make every effort to preserve member privacy, we may need to disclose your Personally Identifiable Information when required by law or if we have a goodfaith belief that such action is necessary to (a) comply with a current judicial proceeding, a court order or legal process served on our website, (b) enforce this Policy or the Terms of Service Agreement, (c) respond to claims that your Personal Information violates the rights of third parties; or (d) protect the rights, property or personal safety of Meetup, its members and the public. You authorize us to disclose any information about you to law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us or you to legal liability."	Privacy Policy	May 23, 2010
MySpace	See Law Enforcement Handbook		
Nexopia	"We will fully cooperate with any request to release information to any law enforcement agency when a proper request is received. We may also take steps to protect the health and well being of members, visitors and other parties if we have reason to believe that any of these persons are in danger.	Privacy Policy	Dec 1, 2012

	Nexopia expressly reserves the right, and in some jurisdictions may be legally required, to report certain materials, such as, but not limited to, child pornography or terror plans, that we may become aware of in the course of providing the Services to the authorities in charge. Some personal information may be stored or processed by third parties, including contractors, business partners and affiliates located in the United States. Therefore, your information may be processed and stored in the United States, and may not be subject to the same privacy rules as in Canada. As a result, the governments, courts, or law enforcement or regulatory agencies may be able to obtain disclosure of your information through laws applicable in the United States. Except as otherwise described in this Privacy Policy, Nexopia.com will not disclose personal information to any third party unless we believe that disclosure is necessary for one of the following reasons: (1) as required by law, including to respond to a subpoena, search warrant or other legal process received by Nexopia.com; (2) to enforce the Nexopia.com Terms of Use or to protect our rights; or (3) to protect the safety of the public and members of Nexopia.com and visitors to the service."		
Ping (Apple)	"It may be necessary − by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence − for Apple to disclose your personal information. We may also disclose information about you if we	Privacy Policy	May 21, 2012

	determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate."		
Pinterest	"Under the heading "What Choices do you Have about your Information?" Close your account at any time. When you close your account, we'll deactivate it and remove your pins and boards from Pinterest. We may retain archived copies of your information as required by law or for legitimate business purposes (including to help address fraud and spam)."	Privacy Policy	Unclear
Plenty of Fish	"We may disclose your information as permitted or required by law. For example, we may be compelled to release information by a court of law or other person or entity with jurisdiction to compel production of such information. If we have reasonable grounds to believe information could be useful in the investigation of improper or unlawful activity, we may disclose information to law enforcement agencies or other appropriate investigative bodies. TERMINATION OF ACCESS TO SERVICE We may, in our sole discretion, terminate or suspend your access to all or part of the Service at any time, with or without notice, for any reason, including, without limitation, breach of this Agreement. Without limiting the generality of the foregoing, any fraudulent, abusive, or otherwise illegal activity that may otherwise affect the enjoyment of the Service or the Internet by others may be grounds for	Terms of Service	Jan 15, 2013

	termination of your access to all or part of the Service at our sole discretion, and you may be referred to appropriate law enforcement agencies. *Service Providers* To provide increased availability of the Website, some of these operations may result in personal information collected by Plentyoffish being stored outside Canada and, as a result, such personal information stored outside of Canada may be accessible to law enforcement and regulatory authorities in accordance with applicable laws of countries outside Canada."		
Reddit	No information provided.		
Tumblr	"Information Disclosed for Our Protection and the Protection of Others: We believe in freedom of expression, and, to the extent reasonable, we try to protect our community from baseless legal demands. That said, we also reserve the right to access, preserve, and disclose any information as we reasonably believe is necessary, in our sole discretion, to (i) satisfy any law, regulation, legal process, governmental request, or governmental order, (ii) enforce this Privacy Policy and our Terms of Service, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues (including exchanging information with other companies and organizations for fraud protection and spam/malware prevention), (iv) respond to user support requests, or (v) protect the rights, property, health or safety of us, our users, any third parties or the	Privacy Policy	Mar 22, 2012

	public in general, including but not limited to situations involving possible violence, suicide, or self harm."		
Twitter	See Law Enforcement Handbook		
Wikimedia Foundation	"Release: Policy on Release of Data It is the policy of Wikimedia that personally identifiable data collected in the server logs, or through records in the database via the CheckUser feature, or through other nonpubliclyavailable methods, may be released by Wikimedia volunteers or staff, in any of the following situations: In response to a valid subpoena or other compulsory request from law enforcement, • With permission of the affected user, • When necessary for investigation of abuse complaints, • Where the information pertains to page views generated by a spider or bot and its dissemination is necessary to illustrate or resolve technical issues, • Where the user has been vandalizing articles or persistently behaving in a disruptive way, data may be released to a service provider, carrier, or other thirdparty entity to assist in the targeting of IP blocks, or to assist in the formulation of a complaint to relevant Internet Service Providers, • Where it is reasonably necessary	Privacy Policy	March 10, 2013

	to protect the rights, property or safety of the Wikimedia Foundation, its users or the public. Except as described above, Wikimedia policy does not permit distribution of personally identifiable information under any circumstances. Registered users are not required to provide an email address. However, when an affected registered user does not provide an email address, the Foundation will not be able to notify the affected user in private email messages when it receives requests from law enforcement to disclose personally identifiable information about the user."		
WordPress.com	"We don't share your personal information with anyone except to comply with the law, develop our products, or protect our rights"		Change log available
WordPress.org	"WordPress.org discloses potentially personally-identifying and personally-identifying information only when required to do so by law, or when WordPress.org believes in good faith that disclosure is reasonably necessary to protect the property or rights of WordPress.org, third parties, or the public at large."		Unclear
World of Warcraft	See Law Enforcement Handbook.		
YouTube (Google)	See Law Enforcement Handbook		
Zynga	No information provided.		

References

Our analysis of lawful access handbooks are available at http://catsmi.ca/resources/public-resources.

Privacy Policies and Terms of Service documents were all collected from companies' public websites, as accessed from a Canadian IP address.

About the Authors

This document was researched and written by Adam Molnar and Christopher Parsons.

Adam Molnar has spent over a decade researching, teaching, and consulting on developments in security and privacy, particularly in the areas of policing, national security, and public safety. He specializes in how collaborative governmental initiatives are arranged, and the privacy and security benefits and challenges that follow. Adam is presently completing his Ph.D in the Department of Political Science at the University of Victoria, is a forthcoming Postdoctoral Fellow in the Surveillance Studies Centre at Queen's University, and is a Principal at BlockG Security and Privacy Consulting. He has published book chapters and policy reports, and he regularly presents his research domestically and further abroad.

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.