Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice

by Colin J. Bennett,[1] Adam Molnar,[2] and Christopher Parsons[3]

Abstract: In this paper we analyze some of the practical realities around deleting personal data on social networks with respect to the Canadian regime of privacy protection. We first discuss the extent to which the European right to be forgotten is, and is not, reflected in Canadian privacy law, in regulation, and in the decisions of the OPC. After outlining the limitations of Canadian law we turn to corporate organizational practices. Our analyses of social networking sites' (SNSes) privacy policies reveal how poorly companies recognize the right to be forgotten in their existing privacy commitments and practices. Next, we turn to Law Enforcement Authorities (LEAs) and how their practices challenge the right because of LEAs' own capture, processing, and retention of social networking information. We conclude by identifying lessons from the Canadian experience and raising them against the intense transatlantic struggle over the scope of the new Draft Regulation.

Prepared for: 2013 Computers, Privacy and Data Protection Conference
Brussels, Belgium
Draft Version 2.1: Please send feedback to cjb@uvic.ca

---

[1] Colin J. Bennett is a professor of political science in the Department of Political Science at the University of Victoria. Hi research focuses on the comparative analysis of surveillance technologies and privacy protection policies at the domestic and international levels.
[2] Adam Molnar is a PhD candidate in the Department of Political Science at the University of Victoria. His research interests focus on the legal, normative, and technical dimensions of digitally mediated surveillance and privacy, particularly in the areas of policing, national security, and public safety governance.
[3] Christopher Parsons is a PhD candidate in the Department of Political Science at the University of Victoria. His research interests focus on how privacy (particularly informational privacy, expressive privacy and accessibility privacy) is affected by digitally mediated surveillance, and the normative implications that such surveillance has in (and on) contemporary Western political systems.

"You may not realize it, but whenever you go online, you're building an identity through the words and images you post and the activities you do. This can become part of your reputation, and it can be a lasting one. Once personal information goes online, it may be difficult to delete. While you may be able to delete it in one place, there may be cached versions or copies stored elsewhere that you cannot control. Digital storage is cheap and computer memory is plentiful--and unlike people, the Net never forgets" (Jennifer Stoddart, Canadian Privacy Commissioner, January 28th, 2011).

Social networking companies' compliance with data retention and disclosure policies is gaining heightened international importance given the European Union's new Draft Regulation. This Draft expands and updates the 1995 Data Protection Directive, and includes the controversial "right to be forgotten" provision. Using this provision, individuals could force an organization to delete personal data stored about them "without delay." Social networks that make such data public will be liable if it is subsequently republished by third-parties, and will be required to "take all reasonable steps, including technical measures" to inform third-parties to delete the information. While the right sounds fine in the abstract, our analysis reveals that "forgetting" is a complicated process. To demonstrate such complexities we turn to Canadian-informed, though broadly North American, experiences to reveal how European aspirations may be thwarted by existing laws, policies, and practices.

Canadians regulators have been mindful of the surveillance potential of major social networking services; the Office of the Privacy Commissioner of Canada (OPC) has investigated both Facebook and Nexopia over their handling, disclosure, and retention of Canadian subscribers' personal information. Government access to social networking data has also become a significant policy issue in the face of tabled 'lawful access' legislation, which would impose data retention and disclosure requirements on telecommunications service providers. In light of the public debate about how social networking information is used by private and public bodies, we have studied how such services operate in Canada as well as their (non-compliance) with Canadian law.

More specifically, we analyze some of the practical realities around deleting personal data on social networks with respect to the Canadian regime of privacy protection. We first discuss the extent to which the European right to be forgotten is, and is not, reflected in Canadian privacy law, in regulation, and in the decisions of the OPC. After outlining the limitations of Canadian law we turn to corporate organizational practices. Our analyses of social networking sites' (SNSes) privacy policies reveal how poorly companies recognize the right to be forgotten in their existing privacy commitments and practices. Next, we turn to Law Enforcement Authorities (LEAs) and how their practices challenge the right because of LEAs' own capture, processing, and retention of social networking information. We conclude by identifying lessons from the Canadian experience and raising them against the intense transatlantic struggle over the scope of the new Draft Regulation.

Is there a "Right to be Forgotten" in Canadian Privacy Law?

The debate surrounding the "right to be forgotten" has largely revolved around the right's scope and its related implications. While the debate is often framed in the context of European versus American values, notably absent have been discussions of how nations

with more rigorous privacy regimes, such as Canada, already do - and do not - instantiate then principles contained in European data privacy policy. In what follows we outline the terms and debates surrounding the proposed Draft Regulation, as related to social networking services, and then identify the limitations of Canadian efforts to influence the practices associated with (predominantly American) social networking services.

The Right to be Forgotten: Current Interpretations

What does the "right to be forgotten" mean? This provision has, to date, proven incredibly controversial and has motivated intense lobbying by US corporations and government agencies. In turning to Article 17 of the current version of the EU Draft Regulation we read:

> The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
>
> a. the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
> c. the data subject objects to the processing of personal data pursuant to Article 19;
> d. the processing of the data does not comply with this Regulation for other reasons. [4]

The Article is included in the inventory of "rights of the data subject" and has intellectual roots in French law, which recognizes *le droit a l'oubli.* The right is not, as was originally proposed, limited to user-generated and -published data; it is broader, relating to any data concerning an individual, even if it has been generated or transmitted by someone else. This has significant implications for data controllers because they are expected to take all reasonable steps to meet individuals' requests, for themselves and for third-parties. Requests must be fulfilled "without delay", though exceptions exist for journalistic and artistic purposes, for complying with legal obligations, and when retained data is needed for proof of accuracy.

Peter Fleischer of Google has contended that this provision contains three interrelated "rights" that progressively threaten freedom of speech. First is the right to erase

[4] "Proposal for a Regulation of the European Union and the Council on the *Protection of Individuals with respect to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*," last modified January 25. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

something that the subject has posted online. This is uncontroversial and is generally recognized in the privacy policies of most SNSes, with varying levels of emphasis and transparency (as we explain below). The "right to be forgotten," at this level, simply requires SNSes to satisfy their stated commitments. The second is the circumstance of another person reposting data generated by the user. If the original user requests the person who reposted to erase, and that person refuses, should a deletion requirement apply to the SNS? Under the proposed Regulation, the answer is likely "yes" unless recognized exceptions applies. The SNS would have the burden of proving such an exception. Third, and most controversially, Article 17 applies to data originally generated by a third-party. Per Fleischer, it appears that these "takedown requests" should also be honored, even for truthful information. Again, the legal burden would lay with a SNS to prove that there is, for example, a legitimate public expression value in keeping the data online.[5] In a subsequent posting, Google explained why it disavowed responsibility for deleting subscriber-created content and why it does not have an obligation to modify search results based on these takedown requests.[6]

Article 17 has precipitated a contest between EU regulators and "Big Data" companies. It has also inspired commentary about the clash between European "protectionist" and American "free speech" values. Jeffrey Rosen asserted that this right is "[t]he biggest threat to free speech on the Internet in the coming decade."[7] To be sure, the implications are more severe for the US, given its lack of a comprehensive data protection regime. For other countries, such as Canada, the proposal exposes a more nuanced set of issues and contrasts.

The Right to be Forgotten in Canadian Privacy Law

Several Canadian privacy laws govern federal/provincial jurisdictions and public/private sectors. Though there are some gaps in coverage, the system has been judged adequate under existing Article 25 provisions of the Data Protection Directive.

Canada's public sector laws require "retention schedules," which should be commonly implemented across federal and provincial government bodies. The Personal Information Protection and Electronic Documents Act (PIPEDA) is the principal legal instrument governing the private sector. Several of its provisions pertain to the "right to be forgotten." Schedule One (4.5) of the legislation states that "[p]ersonal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes." It also requires that organizations "develop guidelines and implement procedures with respect to the retention of personal information" (4.5.2). Furthermore, "personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made

[5] "Foggy Thinking about the Right to Oblivion," Fleischer, Peter, *Peter Fleischer: Privacy...?* March 9, 2011. Accessed October 17, 2012. http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-the-right-to-oblivion.html

[6] "Our thoughts on the Right to be Forgotten," Google Europe Blog, last modified February 16, 2012. http://googlepolicyeurope.blogspot.ca/2012/02/our-thoughts-on-right-to-be-forgotten.html

[7] Jeffrey Rosen, "The Right to be Forgotten," *Stanford Law Review* 64 (2012): 88-92.

anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information" (4.5.3).

Hence, data erasure is not articulated as a right of the data subject but as an obligation of the data controller. Deleting or erasing data that is no longer needed to fulfill identified purposes is seen as a feature of "good" data protection practices and governance, and inextricably linked to questions of whether the data is still needed to meet stated, and identified, purposes. Such an analysis invariably leads to questions about individual consent; in such an analysis another provision (Principle 4.3.8) may apply: "an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and that the organization shall inform the individual of the implications of such withdrawal."

Thus the request to delete personal data can be interpreted as a "withdrawal of consent" and may appear as a legal equivalent to the "right to be forgotten." If there is such a right, however, it only really applies when organizations collect data *about* an individual and retain it longer than required to fulfill identified purposes. Such a right is also interpreted within the larger framework of the "reasonable person" test under what is (essentially) a consent-based statute.

With respect to many corporations operating in Canada, there are practical rather than jurisdictional questions of the extra-territorial reach of Canadian law. Most of the SNSes used by Canadians have, at best, limited physical presences within Canada. In a case involving the US profiling company Accusearch, the Federal Court of Canada insisted that the OPC had jurisdiction over the relevant privacy complaint insofar as a *reasonable and substantial* connection could be found between the entity or the actions complained of, and Canada.[8] Furthermore, the Commissioner's website emphasizes: "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".[9] Today, practical more than jurisdictional questions remain about the OPC's ability to investigate SNS-related complaints.

Canadian Privacy Law and Social Networking

The OPC has investigated Facebook, Google, Netflix, and other US-based companies regardless of their having a physical presence in Canada. In a famous and wide-reaching decision, the OPC asserted that Facebook violated provisions of PIPEDA, including section 4.5.3. The violation related to the confusing distinction between the deactivation of an account and the permanent deletion of data related to an account. The OPC wrote, "[u]nder Facebook's current account deactivation policy, the personal information of users who have deactivated their accounts is retained indefinitely. Indefinite retention is a

[8] "Philippa Lawson v. Accusearch Inc. and Federal Privacy Commissioner," Federal Court of Canada, last modified October 26, 2012, http://reports.fja.gc.ca/eng/2007/2007fc125/2007fc125.html

[9] "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing," Privacy Commissioner of Canada, last modified March 29, 2010, http://www.priv.gc.ca/information/pub/cc_201003_e.asp#toc5

contravention of Principle 4.5 and 4.5.3 [...] a reasonable person would not consider it appropriate for Facebook to continue to retain indefinitely the personal information of a user who has deactivated his or her account and not reactivated it for a long time" [10]. Facebook was asked to implement a retention policy and inform users about it, and to delete personal information linked to deactivated accounts from Facebook's servers after a reasonable length of time. While Facebook did add information about account deletion to its privacy policy it did not develop a retention policy for deactivated accounts.

Jurisdictional issues could not be raised when the OPC investigated a complaint about into the practices of Nexopia, a Canadian SNS directed towards young people. The complaint covered virtually every aspect of Nexopia's practices, including its retention of users' and non-users' personal data. Nexopia admitted to lacking internal policies and procedures for the retention, backup and destruction of its records. The company also confirmed that it retained users' and non-users' personal information in its database and archives since the website's inception in 2003. The OPC wrote that "it is clearly misleading to provide a "Delete Account" option—which states that specific personal information will be deleted—when in fact the information will be retained indefinitely in the website's archive"[11]. Despite most of the complaints being considered "well-founded," Nexopia rejected some of the recommendations on technical grounds.

These interpretations of PIPEDA suggest that Canadians can tell these services to permanently and thoroughly delete their account information, notwithstanding technical difficulties and occasional reasons to retain the data for reasons of law enforcement (see below). Returning to Fleischer's threefold categorization, the right of a user to request the permanent deletion of all user-generated data seems settled, at least in the eyes of the OPC. In this sense, there is a "right to be forgotten" in Canadian law. However, there have yet to be tests of the second and third aspects of this right. Such tests may pose real challenges under Canadian privacy law given that it remains based on a dichotomy between the "individual" and the "organization."

Hence, PIPEDA only goes so far and Canadian citizens are then dependent on the range of ambiguous commitments to deletion, partial-deletion and non-deletion within the corporate privacy policies of largely American companies. As we demonstrate below, these networks' own corporate practices often try to set the terms of how these matters *will* operate, regardless of the guidance provided by federal regulators or national laws.

Organizational Practices and Data Deletion

Canadians are prolific users of social networking services, with 60% of online Canadians – and thus 50% of all Canadians – being members of a social networking service[12]. Our

[10] "Report of the Findings into the Complaint filed by CIPPIC against Facebook Inc.," Privacy Commissioner of Canada, last modified July 16, 2009, http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp#sect7a

[11] "Report of the Findings into the Complaint filed by CIPPIC against Nexopia," Privacy Commissioner of Canada, *(paragraph 58)*, last modified March 1, 2012, http://www.priv.gc.ca/cf-dc/2012/2012_001_0229_e.asp#summary

[12] "Canada's Love Affair with Online Social Networking Continues," *Ipsos Reid,* 2011.

analyses of these services' privacy policies reveal that companies seek to limit jurisdictional review of their practices while establishing company-specific data retention and disclosure policies. The companies also try to limit non-Americans' capacity to restrict the retention and revelation of their personal information. Together, these practices challenge Canadian privacy law and the proposed "right to be forgotten."

Jurisdiction and complaints

Canada's privacy regime has successfully influenced the privacy behaviors of major global social networking companies[13]. Despite the effectiveness of the OPC, however, only one company in our sample, Club Penguin, a Canadian company that was acquired by Disney, specifically states its compliance with Canadian privacy law[14]. Most other social networks (Blizzard[15], Facebook[16], Google[17], LinkedIn[18], LiveJournal[19], MySpace[20], Twitter[21], Zynga[22]) emphasize that they comply with American law, such as Child Online Protection Act, and some with the EU-US Safe Harbour Framework. Several companies stress their compliance with California law (Blizzard[23], Facebook[24], Tumblr[25], Zynga[26]). Nexopia[27], Yahoo!'s Flickr[28], and Instagram[29] all fail to note which privacy laws and international guidelines they will comply with.

These companies often declare the jurisdictions and courts through which all legal proceedings must be conducted. Save for Yahoo![30], Nexopia[31], and Plenty of Fish (a Canadian dating social network)[32], which recognize Canadian courts, all claims must go through either American federal or the state courts of California or New York. Only

---

[13] "Facebook breaches Canadian privacy law: commissioner." Canadian Broadcasting Corporation (CBC), *CBC News: Technology and Science*, July 16, 2009, Accessed October 17, 2012. http://www.cbc.ca/news/technology/story/2009/07/16/facebook-privacy-commissioner.html

[14] "Club Penguin Privacy Policy," Last modified January 11, 2012, http://www.clubpenguin.com/privacy.htm

[15] "Blizzard Entertainment® Online Privacy Policy." Last modified March 25, 2011, http://us.blizzard.com/en-us/company/about/privacy.html

[16] "Facebook Data Use Policy", last modified June 8, 2012, http://www.facebook.com/full_data_use_policy

[17] "Google Privacy Policy," last modified July 27, 2012, http://www.google.ca/intl/en/policies/privacy/

[18] "LinkedIn Privacy Policy," last updated June 16, 2011, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv

[19] "LiveJournal Privacy Policy," last modified December 12, 2010, http://www.livejournal.com/legal/privacy.bml

[20] "MySpace Privacy Policy." Last updated October 1, 2012, http://www.myspace.com/Help/Privacy

[21] "Twitter Privacy Policy," last modified May 17, 2012, http://twitter.com/privacy

[22] "Zynga Privacy Policy," last modified September 30, 2011, http://company.zynga.com/privacy/policy

[23] "Blizzard Entertainment® Online Privacy Policy."

[24] "Facebook Data Use Policy."

[25] "Tumblr Privacy Policy," last modified March 22, 2012, http://www.tumblr.com/policy/en/privacy

[26] "Zynga Privacy Policy."

[27] "Nexopia Privacy Policy," last modified November 2, 2009, http://www.nexopia.com/privacy

[28] "Yahoo! Privacy Policy," last modified April 23, 2010, http://info.yahoo.com/privacy/ca/yahoo/

[29] "Instagram Privacy Policy," last accessed October 28, 2012, http://instagram.com/legal/privacy/

[30] "Yahoo! Privacy Policy."

[31] "Nexopia Privacy Policy."

[32] "Plenty of fish Terms of Use Agreement," Last updated November 2, 2011, http://www.pof.com/terms.aspx

Zynga, a social gaming company, explicitly recognized European jurisdictions, stating that non-US citizens would "agree to submit to the personal jurisdiction of the courts in Luxembourg"[33].

As noted in the previous section, American social networking companies must meet the requirements spelled out in PIPEDA. These requirements, however, have not led all companies to *actually respect and comply with* Canadian law. As demonstrated in our efforts to compel social networking companies to provide subscribers' data - as required under PIPEDA - only a small handful responded at all, and fewer provided data. The most egregious example, Tumblr, stated that it "will not be providing the information you requested. Tumblr is a U.S.-based company with its headquarters in New York. It does not have a corporate presence in Canada and, therefore, it does not fall under the jurisdiction of PIPEDA or Canada's Office of the Privacy Commissioner." In a subsequent follow-up, after we had further explained the company's obligations under PIPEDA, the company reiterated: "We appreciate your interest in engaging in a legal discussion about the scope and reach of PIPEDA, but our prior correspondence stands"[34] The stated requirement to work through New York courts is interesting, given that Tumblr's privacy policy only recognizes the California Civil Code (S. 1798.83-1798.84) and acknowledges that California residents are entitled to ask for information about the categories of subscriber data the company is sharing with affiliates and third-parties.[35]

Individuals may have challenges alerting a social networking company to their concerns about how the company is retaining, processing, or disclosing their personal information. Of our sample, only three companies - Plenty of Fish, Reddit, and World of Warcraft - published their privacy officers' contact information. Most other companies had somewhat ambiguous contact forms or address information. Few companies had clear complaints or resolution processes. This said, two services, LiveJournal and MySpace, recognize the uniqueness of EU subscribers, with the former providing an EU mailing address for complaints and the latter encouraging Europeans to submit questions using the company's online form or by mail. Tumblr also stands out, insofar as the published mailing address is exclusively for California residents. Only Instagram entirely lacked a complaints mechanism though, in subsequent research, we found that its staff was willing to discuss, if not act on, personal information related concerns.

We have asked various SNSes to provide comprehensive records of the information they held on researchers in the course of our work. Few companies have responded to these requests, and those that did either refused to provide any information or failed to comprehensively provide it; while basic data the subscriber generated may have been disclosed, most of associated metadata was not. Given that metadata, in aggregate, constitutes content these companies have arguably failed to fully account for the personally-associated data generated by the users. Tumblr was the only company that both responded and refused to provide data; others, such as Twitter and Facebook, provided data though with limited metadata, whereas Google suggested that data be

[33] "Zynga Privacy Policy."
[34] Michael Sussmann, Personal e-mail with author.
[35] "Tumblr Privacy Policy."

downloaded through their 'Data Liberation Front' toolset. These tools also lack comprehensive metadata information. Such failures to reply and/or comprehensively provide data are significant insofar as they speak to relative unwillingness to fully comply with non-American privacy-related laws.

How social-networking services understand retention and disclosure

Jurisdictional and complaint issues aside, a simple examination of how social networking companies state they retain data is revealing. Google recognizes that, after deleting account information, they may not immediately delete data and that they may not remove data from their backup systems.[36] Such claims are worrying given the long-term retention problems surrounding Street View data insofar as actual retention periods remain ambiguous.[37] While Facebook states that it typically takes a month to delete data - with some information remaining in backup logs up to 90 days - the company's success in actually deleting data, such as photos uploaded to the site, has long been questionable.[38] Companies such as Yahoo! and Foursquare offer commitments similar to those of Facebook. Fourquare also notes that, even after subscribers delete information, "copies of that information may remain viewable elsewhere, to the extent it has been shared with others, distributed pursuant to privacy settings, or copied or stories by other users".[39] Tumblr parallels this statement, informing subscribers that even when deleting their accounts' content, public activity, such as posts that were 'liked' or shared, will remain stored on servers and accessible to the public.[40]

For other services the 'deletion' of subscriber data may largely amount to hiding the information from public viewers. LiveJournal, for example, recognizes that, while individuals can delete their account and accompanying information, data may take an unspecified amount of time to delete and the company may choose to retain the information to the extent necessary to protect the company's legal interests, comply with court orders, et cetera.[41] The inclusion of 'et cetera' leaves open the full range of possible motivations to retain data in contravention of a subscriber's request. In the case of Meetup, the company reserves the right to retain information that the user requests removed if retention is needed to resolve disputes, troubleshoot problems, or enforce the terms of service. Regardless, the company promises, "your information is never completely removed from our databases due to technical and legal constraints (for example, we will not remove your information from our backup stores)"[42]. Nexopia offers similar 'guarantees' as Meetup, insofar as Nexopia states that individuals ought not expect that their personal information will be completed removed from their systems

[36] "Google Privacy Policy."
[37] "Google: Didn't delete Street View data after all," *Yahoo! News*, July 27, Accessed October 17, 2012. http://news.yahoo.com/google-didnt-delete-street-view-data-175540701--finance.html
[38] "Three years later, deleting your photos on Facebook now actually works," Cheng, Jacqui, *Ars Technica*, August 16, 2012, accessed October 17, 2012, http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting/
[39] "Foursquare Labs, Inc. Privacy Policy," last modified July 13, 2012, https://foursquare.com/legal/privacy
[40] "Tumblr Privacy Policy."
[41] "LiveJournal Privacy Policy."
[42] "Meetup Privacy Policy Statement," last modified May 23, 2010, http://www.meetup.com/privacy/

following a deletion request.[43]

Given that many of these services functions as platforms, and thus allow other developers to capture, process, and retain users' generated data, there is the potential for 'deleted' data on the platform (e.g. Facebook, Twitter, LinkedIn, Foursquare) to be retained indefinitely by third-party developers without a way for the platform to enforce a users' deletion request on the third-party. Companies such as Club Penguin, Yahoo!, Google, and Apple[44] reserve the right to share collected or contributed information within and across their corporate organizations, and most social networks include provisos that they 'may' (read: will and do) share information with analytics companies and associated advertisers. Significantly, when we examined the social networking services using Ghostery, a tool that identifies web trackers, we found that all services with the exception of Facebook and Google revealed the presence of third-party analytics and and/or advertising services. Facebook and Google, of course, use their own backend analytics and advertising systems and thus do not need to rely on third-parties for such services.

Organizational implications for 'forgetting'

Current organizational practices may limit the practical instantiation of any right to forget. Few social networking services guarantee that data will, certifiably, be deleted and tend to offer either broad exceptions under which data will be retained or state outright that it *will not* be deleted. Given that most networks let individuals join over the age of 13 join and use the services, this means that youths' personally identifiable information may also be retained indefinitely. Retained data could be retained indefinitely for 'legitimate' business purposes, purposes that the user may have consented to upon accepting the Terms of Service associated with the SNS. Moreover, even if a controller could successfully delete the data from their systems (and, it should be noted, few subscribers will be able to ascertain 'success' given both the lack of access to social networking services' data centers and their common lack of sufficient technical, temporal, and fiscal resources to mount independent forensic investigations) the data may remain in the databases of third-parties associated with the services' development platform. Comprehensive deletion of data held by these third-parties must rely on more than the 'good will' that companies such as Facebook have historically espoused towards their developer community for subscribers to be assured that their data is actually, meaningfully, going to be deleted.[45]

Ultimately, while there is some degree to which subscribers can be 'forgotten' by these services today, successfully being forgotten is muddied by difficulties in ascertaining what data organizations hold on individuals, in networks (not) adhering to relevant and applicable laws, in varying and unclear corporate retention periods, and in the limited capacities for subscribers to scrub data from third-parties that capture, process, or retain their personal information. The challenges facing individuals who seek to enforce their

[43] "Nexopia Privacy Policy."
[44] "Apple Privacy Policy," last modified updated May 21, 2012, http://www.apple.com/privacy/
[45] Katherine Losse, *The Boy Kings: A Journey into the Heart of the Social Network* (New York: Free Press, 2012), 148.

right to be forgotten are compounded when we turn to the law enforcement's appetite for capturing, processing, and retaining social networking data for their own purposes.

Lawful Enforcement Access to Social Networking Services

Social media provides Law Enforcement Authorities (LEAs) a burgeoning stream of information for detecting, preventing, and investigating potentially suspicious activities. Our research reveals how and why Canadian LEAs are using SNSes as proxy organizations to monitor, collect, and retain subscriber data. The circulation of data between SNSes and LEAs further challenge the proposed 'right to be forgotten', insofar as 'forgotten' corporate data may be remembered indefinitely by public bodies.

Information sharing protocols between LEAs and SNSes

Access to private companies' digital records is a common expectation in contemporary law enforcement activities. Every SNS included in our analysis made mention that they will, under certain legal conditions, share information with LEAs or other public authorities. Many, if not all, have some form of 'law enforcement compliance' information that details the types of data available to LEAs, as well as detailed protocols for LEAs to follow to access user data. A small sample of these guides have been made public through leaks or FOIA requests, and they offer insights into the privacy and data management relationships between SNSes and LEAs.

SNSes make a range of information available to LEAs. For example, Facebook will provide authorities with "user contact info" (name, birth date, email address(s), physical address, city, state, zip, phone, registered mobile phone number, work phone, screen name (usually for AOL Messenger/iChat), and website), "group contact info" (a list of users currently registered in a specific group), "user neoprint" (a term for an expanded view of a user profile), "user photoprint" (a compilation of the photos a user has uploaded but not deleted), and "IP logs" (time/date stamps that note when user has logged in, the source IP address, and Internet Service Provider identified with the user Id)[46], [47]. Facebook's security team can also retrieve information for law enforcement that is not explicitly noted in their handbook's description of available data.[48] Similarly, Yahoo!'s compliance guide notes the availability of similar information, such as subscriber information, IP logs, photos, email and other private communication, group content (including email addresses of members), and metadata such as geo-locational information.[49]

For law enforcement, there is often a lag between *requesting* stored communications and SNSes *providing* the requested data. One consequence of this lag have been sharing protocols, typically referred to as 'preservation requests'. Several SNSes, including MySpace, Facebook, Yahoo! (Flickr), and LinkedIn, honour requests from law enforcement to preserve data, typically for up to 90 days. These requests provide

[46] "Facebook Subpoena / Search Warrant Guidelines," Facebook, 2008.
[47] Toronto Police Services, Personal Interview with author, October 5, 2012.
[48] "Facebook Subpoena / Search Warrant Guidelines," p. 7
[49] "Yahoo! Privacy Centre," last modified April 23, 2010, http://info.yahoo.com/privacy/ca/yahoo/

sufficient time for LEAs to assemble necessary legal documents (e.g. subpoenas, court orders, search warrants) to access the preserved data.

Investigative instruments LEAs use to access to social networking data

Canadian LEAs' investigative strategies differ according to whether information is publicly available or is stored on (typically American) servers. In the context of SNSes, publically available information is user generated content that law enforcement can access without court order because it is set to 'public' or 'friend of friend' viewing. Canadian LEAs are increasingly collecting such publicly available data when private information is not required for their investigations.[50] As an example, information is being collected using Facebook search, which provides authorities with publically information from open profiles and public groups. Data collected from such public sources facilitates network-analysis and provides more complete pictures of individuals and their social circles.[51] Interviews that we have conducted have revealed how Facebook's "self-download" feature, ostensibly meant to enhance subscribers' access to their private data, is being used to provide evidence to law enforcement, with one officer referring to this practice as a "best-practice".

Private data is predominantly user generated but is stored privately on a user profile or includes non-publicly viewable metadata that the SNS collects when the user interacts with the service (e.g. geo-locational, facial recognition 'prints'). Where LEAs want access to private data they often first send a (legally) non-binding email requesting the data. When the SNS asks for, or requires, LEAs to submit requests using formal legal documents then either domestic or international legal instruments are used. Many American SNSes (e.g Facebook, Google, and Twitter) explicitly honour Canadian court orders if they present an "equivalent authority"[52] to US court orders or administrative subpoenas ; Interview with Vancouver Police Department 2012). In Canadian law, production orders are used to request and compel communication records from SNSes. In the case of Facebook, their Ontario office functions as their Canadian hub for lawful access requests. Per Canadian legal requirements, such requests to this office must come from Ontario-based LEAs. Consequently, non-Ontario LEAs must be "backed" by Ontario officials[53]. These cross-provincial jurisdictional difficulties may be 'remedied' by Canada's proposed 'lawful access' legislation. Proponents of the legislations claim that the legislation will bolster the use and effectiveness of production orders by removing provincial jurisdictional barriers and creating new production orders to capture "traffic data" and "subscriber and/or service provider information"[54], though critics argue the legislation will instead facilitate SNS-linked 'fishing expeditions' and be used to

[50] "Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities," Public Safety Canada, August 2011, last accessed on October 28, 2012, http://www.sfu.ca/iccrc/content/PS-SP-socialmedia.pdf
[51] "Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities."
[52] "Facebook Subpoena / Search Warrant Guidelines," Facebook, 2010.
[53] Vancouver Police Department, Personal Interview with author, October 10, 2012.
[54] "Lawful Access -- Consultation Document," Department of Justice, last modified August 3, 2012. http://justice.gc.ca/eng/cons/la-al/d.html

massively monitor Canadians.[55]

While Canadian production orders are accompanied by judicial authorization, the orders are not always respected by SNSes[56]; in such cases LEAs can use Mutual Legal Assistance Treaties (MLATs) to retrieve information stored on US servers. MLATs facilitate cooperation between LEAs of different countries, and outline jurisdictional territories, associated investigative protocols, and conditions of sharing information and physical evidence linked to the particular investigation. Canadian LEAs initiate MLATs so that American authorities can compel American-based SNSes to preserve and provide data sought by the Canadians. While the MLAT process may result in the disclosure of US-based data, they are a cumbersome legal instrument and take from 6-8 months to "as long as never"[57] to complete. The lengthy processing times and jurisdictional challenges involved with lawful access to "private" user information through MLAT processes has placed a premium on acquiring as much SNS subscriber information using domestic - open source and legal instrument - methods.

Data Management and Policing Operational Databases in Canada

Contemporary criminal justice practices largely depend on the efficacy of digital information management systems. LEAs want to build pictures of suspicious activity over time, from "pre-crime" to "post-crime." Consequently, information and data retention are integral to the stated intent to "detect, prevent, and investigate" such activity. Canada's national police rely on two primary operational databases to provide digital storage and access of information related to their investigations, the Canadian Police Information Centre (CPIC) and the Police Reporting and Occurrence System (PROS). CPIC holds more than "10 million records and processed more than 200 million queries through 40,000 access points in 2009". PROS is a "records management system containing information on individuals who have come into contact with police, either as a suspect, victim, or offender" and is meant to "record all aspects of an investigation"[58]. PROS integrates the RCMP with 23 police partner agencies and processes about 1.6 million occurrence files per year. Significantly, the PROS database mandate would permit the collection, retention and sharing of public and non-public information gleaned from SNSes. CPICs rigid data structures, on the other hand, limit the integration of such information.

A recent audit of these databases found that "the RCMP had yet to formally establish MOUs with approximately 25% of the police agencies that access CPIC" and consequently could not prevent several agencies from disseminating details on "convictions, discharges, or pardons to employers without the informed consent of the prospective employee".[59] An audit of the PROS database reflected that, though a

---

[55] "Canadian Social Media Surveillance: Today and Tomorrow," Parsons, Christopher, *Technology, Thoughts, and Trinkets*, May 28, 2012, accessed January 27, 2013, http://www.christopher-parsons.com/blog/technology/canadian-social-media-surveillance-today-and-tomorrow/

[56] Vancouver Police Department, Personal Interview with author, October 20, 2012.

[57] Fenton, Mark. Personal Interview with author, October 2012.

[58] "Audit of Selected RCMP Operational Databases," Privacy Commissioner of Canada, 2011 http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_rcmp_2011_e.asp, p. 7

[59] "Audit of Selected RCMP Operational Databases," p. 4

comprehensive privacy policy and set of operating procedures existed, serious problems concerning management of, and access to, the data persisted. Specifically, the OPC found that personal information was being held in the PROS for longer than allowable under the Canadian Privacy Act. Further, the RCMP could not prove that they performed the necessary reviews to guarantee that policies governing personal information in the database were being met. As a result, if misuse of the database to occur, it would be difficult to investigate transgressions.[60]

The retention and circulation of data captured through non-EU law enforcement and other security authorities on EU citizens undermines the ideological underpinnings, and practical instantiation, of the right to be forgotten. Even if SNS organizations comply with the EU proposal and delete data from *their* databases, the issue of collection, retention and dissemination of citizens' data to non-EU public bodies would persist. Consequently, while personal information may be inaccessible to fellow citizens, LEAs may retain, circulate, and process this information without the citizen's knowledge. The practical implications of the collection and retention of data by not only Canadian LEAs, but all non-EU public bodies, undermines any hope that the right to be forgotten will be a comprehensive right; instead, it might better be understood as a right to be quasi-forgotten, with 'forgetting' being dependent on the circumstances and particularities associated with each subscriber's account.

Conclusion

The current debate about the 'right to be forgotten' has generally been framed as a clash between American and European values. This framing tends to see the problem as a false dichotomy. The "Net never forgets" as Jennifer Stoddart stated in the epigraph to this paper, but our analysis of the major SNSes operating in Canada demonstrates that forgetting occurs along a multi-dimensional continuum. At a policy level, there are commitments to deletion, partial deletion, and non-deletion. None of these practices constitutes 'forgetting.' Rarely, has a SNS committed to the total and thorough erasure of all data relating to users. Even more rarely has that erasure occurred. Those commitments and non-commitments may, or may not, be reflected in actual organizational practices and technical capabilities.[61]

A distinction must be made between what a social network service forgets, and forgetting social networking information. Thus, when Facebook, for example, deletes your information, the RCMP does not do the same. Deletion is not the same as "forgetting." Deletion takes place in the context of powerful institutional expectations, motivations, and legacies. The privacy policies we surveyed reveal that companies each engage in a process of "quasi-forgetting," where promises of erasure or deletion are hedged by a number of conditions relating to the timing of the deletion, the inability to guarantee the behavior of third-parties (including law enforcement), the need to retain for unspecified legal purposes, the technical complexities, and the realities of data analytics. "Quasi-

[60] "Audit of Selected RCMP Operational Databases."

[61] For another detailed review, see "The Right to be Forgotten Across the Pond," Ambrose, M. and Ausloos, J. Paper presented at the *Telec*ommunications Policy Research Conference, September 21, 2012. Accessed online, October 20, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032325

forgetting", therefore, is reflected in the following rhetorical devices:

- Forgetting: but not yet
- Forgetting: but only for what we deem to be PII
- Forgetting: but not information that your friends have said or shared about you
- Forgetting: but only for us, not for others
- Forgetting: but we need to cover our legal backs
- Forgetting: but we cannot guarantee complete erasure
- Forgetting: but not for third-party analytics

These exceptions and qualifications are readily apparent, and often readily admitted to. They constitute the "known unknowns." Beyond these, there may be a range of unintended effects of personal data retention within a social-networking environment that are even less understood and controlled for -- the "unknown unknowns" of networked communications. Our analysis suggests that the legal and policy dilemmas that have shaped the international debates about the 'right to be forgotten' require a more nuanced appreciation of current erasure and deletion practices. Not adopting a nuanced understanding of the organizational, legal, and practical realities that stand between establishing the right and instantiating it in practice could undermine the EU's work on this topic. As such, it behoove EU regulators to move beyond the EU-US debate and consider how other privacy regimes are addressing deletion and forgetting requirements on social networks. Failure to learn from these regimes' policy processes risks plunging the EU into a rugged, and as yet unresolved, quagmire where corporate and public policies contest the implementation of privacy legislation meant to target, typically American, social networking services.

WORKS CITED

Ambrose, M. and Ausloos, J. "The Right to be Forgotten Across the Pond." Paper presented at the *Telec*ommunications Policy Research Conference, September 21, 2012. Accessed online, October 20, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032325

Apple. "Apple Privacy Policy." Last modified May 21, 2012. http://www.apple.com/privacy/

Blizzard Entertainment. "Blizzard Entertainment® Online Privacy Policy." Last modified March 25, 2011. http://us.blizzard.com/en-us/company/about/privacy.html

Canadian Broadcasting Corporation (CBC). "Facebook breaches Canadian privacy law: commissioner." *CBC News: Technology and Science*, July 16, 2009. Accessed October 17, 2012. http://www.cbc.ca/news/technology/story/2009/07/16/facebook-privacy-commissioner.html

Cheng, Jacqui. "Three years later, deleting your photos on Facebook now actually works," *Ars Technica*, August 16, 2012. Accessed October 17, 2012. http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting/

Club Penguin. "Privacy Policy." Last modified January 11, 2012. http://www.clubpenguin.com/privacy.htm

Department of Justice. "Lawful Access -- Consultation Document." Last modified August 3, 2012. http://justice.gc.ca/eng/cons/la-al/d.html

Der Speigel Online, "US Lobbyists Face off with EU on Data Privacy Proposal," October 17, 2012. http://www.spiegel.de/international/business/us-government-and-internet-gi

European Union (EU). Proposal for a Regulation of the European Union and the Council on the *Protection of Individuals with respect to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Published January 25, 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Facebook. "Facebook Subpoena / Search Warrant Guidelines." 2008.

Facebook. "Facebook Subpoena / Search Warrant Guidelines." 2010.

Facebook. "Data Use Policy." Last modified June 8, 2012. http://www.facebook.com/full_data_use_policy

Federal Court of Canada. "Philippa Lawson v. Accusearch Inc. and Federal Privacy Commissioner." Last modified October 26, 2012. http://reports.fja.gc.ca/eng/2007/2007fc125/2007fc125.html

Felt, Adrienne, and David Evans. "Privacy Protections for Social Networking Platforms." Paper presented at the Workshop for Web 2.0 Security and Privacy, Oakland, CA, 22 May 2008.

Fenton, Mark. Personal Interview with author. October, 2012.

Fleischer, Peter. "Foggy Thinking about the Right to Oblivion," *Peter Fleischer: Privacy...?* March 9, 2011. Accessed October 17, 2012. http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-the-right-to-oblivion.html

Foursquare. "Foursquare Labs, Inc. Privacy Policy." Last modified July 13, 2012. https://foursquare.com/legal/privacy

Google. "Our thoughts on the Right to be Forgotten," *Google Europe Blog*, February 16. 2012. Last accessed October 20, 2012. http://googlepolicyeurope.blogspot.ca/2012/02/our-thoughts-on-right-to-be-forgotten.html

Google. "Privacy Policy." Last updated July 27, 2012. http://www.google.ca/intl/en/policies/privacy/

Instagram. "Privacy Policy." Last updated August 30, 2012. http://instagram.com/about/legal/privacy/

Ipsos Reid. "Canada's Love Affair with Online Social Networking Continues," Ipsos Reid, 2011.

LinkedIn. "Privacy Policy." Last modified June 16, 2011. http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv

LiveJournal. "LiveJournal Privacy Policy." Last modified December 12, 2010. http://www.livejournal.com/legal/privacy.bml

Losse, Katherine. *The Boy Kings: A Journey into the Heart of the Social Network* (New York: Free Press), 2012.

Meetup. "Meetup Privacy Policy Statement." Last updated May 23, 2010. http://www.meetup.com/privacy/

MySpace. "Privacy Policy." Last updated October 1, 2012. http://www.myspace.com/Help/Privacy

Nexopia. “Privacy Policy.” Last updated November 2, 2009. http://www.nexopia.com/privacy

Parsons, Christopher. “Canadian Social Media Surveillance: Today and Tomorrow,” *Technology, Thoughts, and Trinkets*, May 28, 2012, accessed January 27, 2013, http://www.christopher-parsons.com/blog/technology/canadian-social-media-surveillance-today-and-tomorrow/

Plenty of Fish. “Plenty of fish Terms of Use Agreement.” Last updated November 2, 2011. http://www.pof.com/terms.aspx

Privacy Commissioner of Canada. *Report of the Findings into the Complaint filed by CIPPIC against Facebook Inc.* July 16, 2009. http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp#sect7a

Privacy Commissioner of Canada. *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing.* Last modified March 29, 2010. http://www.priv.gc.ca/information/pub/cc_201003_e.asp#toc5

Privacy Commissioner of Canada. *Report of the Findings into the Complaint filed by CIPPIC against Nexopia.* Last modified March 1, 2012. http://www.priv.gc.ca/cf-dc/2012/2012_001_0229_e.asp#summary

Public Safety Canada. *Social Media Sites: New Fora for Criminal, Communication, and Investigation Opportunities*, August 2011, last accessed on October 28, 2012, http://www.sfu.ca/iccrc/content/PS-SP-socialmedia.pdf

Rosen, Jeffrey. 2012. “The Right to be Forgotten.” *Stanford Law Review* 64 Stan. L. Rev. Online: 88-92.

Stoddart, Jennifer. “The Net Never forgets: Remember to Protect Personal Data,” Website of the *Office of the Privacy Commissioner of Canada*, January 28, 2011. Accessed October 17, 2012. http://www.priv.gc.ca/resource/dpd/2011/index_e.asp

Tumblr. “Privacy Policy.” Last updated March 22, 2012. http://www.tumblr.com/policy/en/privacy

Twitter. “Twitter Privacy Policy.” Last updated May 17, 2012. http://twitter.com/privacy

Vinograd, Cassandra and Raphael Satter. “Google: Didn’t delete Street View data after all,” *Yahoo! News*, July 27. Accessed October 17, 2012. http://news.yahoo.com/google-didnt-delete-street-view-data-175540701--finance.html

Yahoo! “Yahoo! Privacy Centre.” Last updated April 23, 2010. http://info.yahoo.com/privacy/ca/yahoo/

Zynga. “Privacy Policy.” Last updated September 30, 2011. http://company.zynga.com/privacy/policy