Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies

Colin J. Bennett, Christopher A. Parsons and Adam Molnar

2014

This article was originally published at:
http://www.jlisjournal.org/

Real and Substantial Connections: Enforcing Canadian Privacy Laws Against American Social Networking Companies

COLIN J BENNETT[*], CHRISTOPHER A PARSONS AND ADAM MOLNAR

Abstract

Any organisation that captures personal data in Canada for processing is deemed to have a 'real and substantial connection' to Canada and thus fall within the jurisdiction of the Personal Information Protection and Electronic Documents Act (PIPEDA) and of the Office of the Privacy Commissioner of Canada (OPC). What has been the experience of enforcing Canadian privacy protection law on US-based social networking services? We analyse some of the high-profile enforcement actions by the Privacy Commissioner. We also test compliance through an analysis of the privacy policies of the top 23 SNSs operating in Canada and through the use of access to personal information requests. Our analysis suggests that non-compliance is widespread, and is explained by the countervailing conceptions of jurisdiction inherent in corporate policy and technical system design.

Introduction

Canadian influence over global privacy and data protection standards has been, and remains, important. The former Federal Privacy Commissioner, Jennifer Stoddart, has been widely praised for her international leadership on the issue. Furthermore, Canadian regulators have had some success in enforcing compliance with Canadian privacy law against some of the largest information brokers, including Google and Facebook. In a speech in 2011, the Assistant Privacy Commissioner, Chantal Bernier, attributed Canadian leadership in this area to Canada's hybrid privacy regime, its bilingualism, its bijurism (the blend of common law and civil law traditions), its multiculturalism, and to the independence of its provincial and federal information and privacy commissioners.[1]

At the same time, the Canadian privacy regime is now increasingly pressured by the internationalisation of data collection, sharing, and retention, particularly by social networking services (SNSs), which are largely based in the United States. Canadians are prolific users of SNSs, with 60 per cent of

[*] Department of Political Science, University of Victoria, Victoria, BC Canada. <cjb@uvic.ca>; <www.colinbennett.ca>.

[1] Chantal Bernier, 'Canada's Role and Influence in the Global Privacy Arena' (Address delivered at the AccessPrivacy[HB] Conference, Toronto, 3 June 2011) <http://www.priv.gc.ca/media/sp-d/2011/sp-d_20110603_cb_e.asp>.

online Canadians — and thus 50 per cent of all Canadians — being members of a social networking service, broadly defined.[2] This relationship can be seen as another chapter in an ongoing narrative of Canada serving on the 'front line' of privacy, given the nation's geographic, economic, and political proximity to the United States. But while Canada's experiences surrounding data protection are domestically interesting they can also hold broader lessons for other countries as well.

In this paper we address the question: how do SNSs, which are predominantly situated in the United States, and therefore under the jurisdiction of American law, respond to efforts to enforce Canadian privacy protection law? And what lessons can be derived from the Canadian experience? The development of Canadian privacy law has been heavily influenced by considerations of extra-territoriality, both within Canada and beyond. As we show below, it is now established that any corporation that captures the personal data of Canadians within Canada, regardless of having a physical presence or employees within the country, must comply with Canadian privacy law if there is a 'real and substantial connection to Canada.' The extra-territorial impact of Canadian law is established through a series of decisions under Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* ('*PIPEDA*').

After examining the legal dimensions of privacy in Canada we explore the corporate practices and technical capabilities related to data accessibility and retention. Here, we focus on how corporations differentially assert how and when they comply with non-domestic (ie non-US) laws, and how technical restrictions may stymie compliance with foreign privacy laws. In effect, corporate and technical practices bring about their own challenges in applying non-American law to the practices of American data brokers. We argue that there are, in fact, three sets of rules (legal, corporate and technical) all of which need to be in alignment in the online social networking environment.

Our analysis is based on a review of the privacy policies of the major social networking companies operating in Canada.[3] In this paper, we are specifically interested in questioning *whether* and *how* these SNSs claim that they are compliant with certain international and/or national privacy standards. With which laws do these networks think they need to comply? In addition to an analysis of privacy policies, we also present the results of some tests of the extent to which SNSs believe that they are obliged to honour access requests for Personally Identifiable Information (PII) under Canadian law. Common

---

2 Ipsos Reid, *Canada's Love Affair with Online Social Networking Continues* (2011) <http://www.ipsos-na.com/news-polls/pressrelease.aspx?id=5286>.

3 This project is supported by a grant from the Contributions Program of the Office of the Privacy Commissioner. We are grateful to Brittany Shamess and Michael Smith for research assistance. The full results of our research are presented at: <www.catsmi.ca>.

letters of access for both user-generated data and metadata were sent to a sample of these companies. We present some of the initial responses.

While the policy landscapes between the Canadian and other privacy regimes manifest in different ways, all privacy and data protection regulators share a common set of pressing legal and normative challenges over cross-jurisdictional data protection enforcement. With this in mind, we conclude with some more general reflections about the tensions between legal jurisdiction and 'applicable laws,' and the corporate and technical dimensions of jurisdiction revealed in this paper.

1 *The Evolution and Profile of Canadian Information Privacy Law*

Canadian privacy protection policy has developed a distinct profile. For the public sector, the first privacy legislation at the federal level was contained in Part IV of the 1977 *Canadian Human Rights Act*, which established the office of the Privacy Commissioner as a member of the Canadian Human Rights Commission. The Commissioner's main task was to receive complaints from the general public, conduct investigations and make recommendations to Parliament. Parallel debates over a federal *Access to Information Act* in the early 1980s raised a range of issues about the compatibility between such legislation and the privacy standards within Part IV. The current federal *Privacy Act*,[4] which has not been substantively revised since 1982, flows from a belief that data protection should be a corollary to freedom of information, and that the various exemptions in both pieces of legislation should be internally consistent. Thus was institutionalised the Canadian innovation of legislating access to information and privacy protection within the same statutory framework. This model was later copied by the provinces, all of which now have in place access to information and privacy protection laws for public agencies, as well as by a few foreign jurisdictions, such as Hungary.

None of this legislation, however, applies to the private sector. The passage in 1993 of Quebec's Bill 68, *An Act respecting the protection of personal information in the private sector*, gave effect to the information privacy rights incorporated in the Quebec Civil Code.[5] As a result of passing this legislation, Quebec became the first jurisdiction in North America to produce comprehensive data protection rules for commercial organisations. In the rest of Canada there were only a few isolated statutes related to specific sectors, such as the consumer credit industry, and certain common law remedies and constitutional provisions of potential relevance. For the most part, privacy

[4] *Canada Privacy Act*, RSC 1985, c P-21 <http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html>.

[5] Quebec, *An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1 <http://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html>.

protection in the private sector was largely dependent on the application of a set of voluntary codes of practice developed according to the framework of the 1981 OECD Guidelines for the Protection of Personal Information.[6]

Throughout the 1990s, a number of political, international, technological and legislative developments convinced federal policy makers that this incoherent policy could not continue. First, the passage of the EU Data Protection Directive in 1995 meant that no jurisdiction in Canada (save Quebec) could plausibly claim an 'adequate level of protection', thus restricting which provinces could safely process personal data transmitted from EU member states.[7] Second, the passage of the Quebec legislation created an 'unlevel playing field' within the Canadian federation, creating uncertainties and transaction costs for businesses that operated in different provinces. Third, the commercialisation of some governmental functions had undermined the implementation of public sector data protection law and the ability of Canada's privacy commissioners to ensure the protection of personal data when it is transferred to a private contractor. Finally, the debates over the development and character of what was then called the 'information (super)-highway' exposed the need for a common set of 'rules of the road' for the networked and distributed computing and communications environment of the 21st century.[8]

The result of the subsequent government commitments, policy analysis and legislative debate was the *PIPEDA*, which came into force on 1 January 2001.[9] With this legislation, Canada took a significant step towards providing a more complete set of privacy rights for its citizens.[10] Initially, the law only applied to the banks, telecommunications, broadcasting, airlines, and transportation companies, as well as to companies that transferred personal information across provincial or international borders for a commercial purpose.

After three years, the law applied to all commercial activities by the private sector, including companies under provincial or territorial jurisdiction, unless they were already covered by a 'substantially similar' provincial or territorial

---

6 Organization for Economic Cooperation and Development (OECD), *Guidelines for the Protection of Personal Information and Transborder Data Flows* (OECD, 1981).

7 *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ No L281.

8 Colin J Bennett, 'Rules of the Road and Level-Playing Fields: The Politics of Data Protection in Canada's Private Sector' (1996) 62(4) *International Review of Administrative Sciences*.

9 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

10 The law is based on the privacy code of practice negotiated under the auspices of the Canadian Standards Association: *Model Code for the Protection of Personal Information* Q-830 (CSA, 1995).

law. The federal government had already declared the 1993 private sector legislation in Quebec as meeting this standard. As of 2013, only BC and Alberta have passed omnibus private sector legislation, although some provincial laws governing health information have also been declared substantially similar. In all other provinces, including Ontario, *PIPEDA* applies by default.

So when examining the overall profile of Canadian privacy legislation it is important to understand how the rules and regulations vary across both federal and provincial jurisdictions, *and* public and private sectors. The entire privacy regime has evolved pragmatically in general conformity with internationally agreed 'fair information practices.' However, there are still a few gaps and inconsistencies. Significantly, the extra-territorial dimensions and impacts of privacy legislation have been a prominent concern from the outset in Canada and between Canada and other countries. That history has legacies for the contemporary attempts to apply Canadian privacy protection principles beyond Canadian borders.

2 *Legal Jurisdictions: The Extra-Territorial Reach of PIPEDA*

In terms of the behavior of organisations based in Canada, the extra-territorial reach of *PIPEDA* is expressed within s 4.1.3 of Schedule One of the Act:

> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.[11]

This provision in *PIPEDA* applies if the 'third party' is outside Canada, regardless of whether the organisation resides in a jurisdiction with equivalent privacy protection law. The Canadian approach, of requiring specific contractual or other guarantees, is often held up as an alternative to the international data flow restrictions inherent within the EU Directive. Unlike the EU position, Canada's approach to data protection reflects an 'organization to organization' approach instead of a 'country to country' approach.[12] However, it is important to acknowledge the relative limitations of the Canadian approach: it tends to apply only in situations where the transfer takes place just for the 'processing' of personal data collected in Canada. The OPC is clear that such a transfer is considered a 'use' rather than a 'disclosure'; in the case of disclosure, additional consent would normally be

[11] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 4.1.3.

[12] Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders* (January 2009) <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp>.

required for the transfer.[13] In other words, the responsible organisation would then be responsible and liable for any breach of *PIPEDA* by that third party, wherever it resides.

How then does *PIPEDA* apply to the capture of information about Canadians by organisations that have no "physical presence" (in terms of corporate offices and/or employees) in Canada? The extra-territorial reach of Canadian law rests on what has come to be called the 'real and substantial connection to Canada' test, first articulated by the Supreme Court in 1995,[14] and which now involves a complicated multi-step inquiry. The onus is always on the party seeking to have the action determined in the Canadian court to establish presumptive jurisdiction. This requires an analysis of the 'real and substantial connection' between that court and the claim. If a Canadian court were to assume jurisdiction, the question shifts from one of the existence of jurisdiction to that of the exercise of jurisdiction. At this point, the party challenging the jurisdiction of the Canadian court must demonstrate why a proposed foreign forum would be a more appropriate arena to consider the claim. That determination may vary depending on the contexts of each case.[15]

The law involving the 'real and substantial connection' to Canada is complex and evolving. This said, the Canadian courts have expressed a view that if a business captures personal information about Canadians in Canada, it must comply with *PIPEDA*, regardless of whether it has a physical presence in Canada. This interpretation of *PIPEDA* has been shaped by a case involving a US company, Accusearch, which offered background searches on individuals including criminal record checks and psychological profiles. Phillipa Lawson, then of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), applied for her profile from the company. Subsequently she lodged a complaint with the Office of the Privacy Commissioner of Canada (OPC) that alleged the company was engaged in the non-consensual collection, use and disclosure of personal data in violation of *PIPEDA*.

In response, the OPC opened an investigation into the company's practices. Accusearch did not cooperate with the investigation and failed to provide the names of Canadian-based sources of their data. Given the company's US residency, combined with their refusal to disclose whether data sources originated from a Canadian source, the OPC asserted that it had no power to investigate the company on the basis that it lacked a physical commercial presence in Canada. The Commissioner took the view that normally 'Canadian legislation will only apply to the persons, property, juridical acts and events that reside within the territorial boundaries of the enacting body's

[13] Ibid.

[14] *Libman v Queen* [1985] 2 RSC 178.

[15] *Club Resorts Ltd v van Breda* [2012] SCC 17.

jurisdiction.'[16] On the basis of the company lacking a Canadian presence, the Commissioner could not compel the company to respond.

On appeal from the complainant, the Federal Court of Canada disagreed with the OPC's interpretation and concluded that the Commissioner had jurisdiction to investigate the complaint, despite any practical difficulties in carrying out an effective investigation. The Judge went on to find that the Privacy Commissioner had jurisdiction over the subject matter of the complaint (the collection, use and disclosure of personal information) and over the person insofar as a reasonable and substantial connection could be found between the entity or the actions complained of and Canada: 'PIPEDA gives the Privacy Commissioner jurisdiction to investigate complaints relating to the cross-border flow of personal information.'[17] We are not aware of any other country in which a court has asserted an extra-territorial jurisdiction for domestic privacy law, if they see little or no prospect of their decisions begin enforced.

Armed with the powers provided by the Canadian Federal court, the OPC reopened its own investigation. Based on information provided by the Federal Trade Commission, which had launched a separate investigation, the Commissioner found that the company had indeed breached *PIPEDA* on a number of counts. The OPC has asserted that:

> This is an important step in international co-operation and collaboration that will become increasingly necessary to adequately protect privacy rights on both sides of the border in years to come. The collaborative efforts of the OPC and the FTC in this case have enhanced and ensured consistency in approach between the two jurisdictions.[18]

The precedent for cooperation and coordination was thus established. In 2010, the effort to collaborate with non-Canadian data protection authorities took a further step with the establishment of the Global Privacy Enforcement Network (GPEN). [19] The network currently comprises authorities from twenty-four different countries, including the United States.

Furthermore, the Accusearch decision allowed the OPC to assert the extra-territorial reach of *PIPEDA* in some other key cases. In one of the more famous and wide-reaching decisions issued by any data protection authority,

---

[16] Office of the Privacy Commissioner of Canada, Report of Findings, *Complaint under PIPEDA against Accusearch Inc., doing business as Abika.com* (2009) <http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_e.asp>.

[17] *Philippa Lawson v Accusearch Inc and Federal Privacy Commissioner* [2007] FC 17 <http://reports.fja.gc.ca/eng/2007/2007fc125/2007fc125.html>.

[18] Office of the Privacy Commissioner of Canada, *PIPEDA Case summary 2009-009* (2009) <http://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp>.

[19] Global Privacy Enforcement Network (2013) <www.privacyenforcement.net>.

the OPC announced in July 2009 that Facebook had violated various provisions of *PIPEDA*. Facebook initially resisted the question of jurisdiction — and, at the time, lacked physical offices in Canada — but finally cooperated (without prejudice) in the investigation and made changes to its products as a result of the OPC's investigation report and subsequent audits.[20] Since 2009 the company has opened Canadian offices and, in 2011, the OPC began another investigation addressing online tracking linked to 'Like buttons' and 'social plug-ins.' The investigation was finally concluded in 2012, after a lengthy and resource-intensive process.

Working with foreign regulators, the OPC has successfully enforced Canadian privacy law on other American companies. In 2010 the Commissioner partnered with the Federal Trade Commission to investigate Google's 'Buzz' product and, more recently, in 2013 collaborated with the Dutch Data Protection Authority. This latter case saw the regulators find against WhatsApp, a California-based company, on grounds that the company non-consensually accessed and used users' contact lists and that the information transferred was excessive and retained for longer than necessary. The company cooperated with both offices and changed some of its practices according to the recommendations. It is also noteworthy that the complaint, in the Canadian case, was initiated by the OPC pursuant to s 11(2) of *PIPEDA*, which lets the Commissioner initiate a complaint if there are 'reasonable grounds.'[21]

Subsequently, the Commissioner has explicitly reaffirmed her jurisdiction over cloud computing services. The OPC's website states:

> 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.[22]

The Commissioner's position parallels that outlined in a study the OPC commissioned in 2008 about the virtual world, Second Life. In the study, the author reaches the following finding:

---

[20] Office of the Privacy Commissioner of Canada, 'Privacy Commissioner: Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features' (News Release, 4 April 2012) <http://www.priv.gc.ca/media/nr-c/2012/nr-c_120404_e.asp>.

[21] Privacy Commissioner of Canada, *Report of the Findings Investigation into the Personal Information Handling Practices of WhatsApp Inc (2013)* <http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp>.

[22] Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing* (2013) <http://www.priv.gc.ca/information/pub/cc_201003_e.asp#toc5>.

> Linden Lab, by operating Second Life, is conducting a commercial activity. Linden Lab collects personal information of Second Life account holders and uses this personal information for the purpose of operating Second Life. Canadians have registered accounts on Second Life. PIPEDA grants the Privacy Commissioner of Canada jurisdiction to investigate foreign organizations in their dealings with the personal information of Canadians, thus PIPEDA applies to Second Life and Linden Lab.[23]

In summary, from the OPC's point of view, the law is relatively clear, even though there might be practical and resource difficulties in investigating a complaint focused on foreign-based services. The OPC's position on cloud computing, combined with earlier successful assertions of Canadian law over American social networking companies, confirms that these companies indeed have 'real and substantial connections' between their operations and Canadian citizens.

What, then, do major companies operating in Canada say about the appropriate jurisdiction for their operations? When confronted with an assertion of rights by Canadian data subjects, how do they respond? To respond to these questions we turn to companies' privacy policies and their statements of jurisdiction, as well as to tests of compliance with access to requests for personal information.

3 Corporate 'Jurisdictions': Privacy Policies and Terms of Service

In this section, we turn to the respective companies' terms of service and privacy policies. In the course of our research we have surveyed the top 23 SNSs used in Canada and analyzed them according to a range of questions relating to: the content and visibility of the policy; the procedures for the data subject (in terms of exercising privacy rights); the claims about the definition and capture of PII; the disclosure of PII to other organisations including law enforcement; commitments about security; and commitments about access and correction rights. Appendix One summarises the national privacy laws, international guidelines, or self-regulatory mechanisms with which these companies state compliance.

Our analysis contributes to the lengthy body of literature based on the analysis of privacy policies.[24] Stated privacy commitments have regulatory

---

[23] Janet Lo, *Second Life: Privacy in Virtual Worlds* (2008) <http://www.priv.gc.ca/information/pub/sl_080411_e.asp#sec32ds>.

[24] Irene Pollach, 'What's Wrong with Online Privacy Policies?' (September 2007) 50(9) *Communications of the ACM* 103; Aleecia M McDonald and Lorrie Faith Cranor, 'The

consequences insofar as a proven contrast between a stated commitment and an actual practice can provide *prima facie* evidence of deception. The complex and lengthy legalese that we then see in most privacy policies is, therefore, a reflection of a perceived need for a legal precision that almost invariably confuses and mystifies the average consumer.[25] 'Layered' privacy policies are, therefore, generally advised that move from simple, short-form versions through a series of steps to the longer, and more legally precise, versions.

Many, though not all, of the SNSs in our survey claimed compliance with at least one privacy protection regime. Notably, however, Flickr (Yahoo!), Instagram, Meetup, Nexopia, Reddit, Wikimedia Foundation, and Wordpress all failed to mention compliance with any specific national or international regime. Despite the OPC's high-profile engagements with foreign social networks such as Facebook, only one company in our sample, Club Penguin, a Canadian company acquired by Disney, specifically states its compliance with Canadian privacy law.[26]

Most other social networks, including Blizzard,[27] Facebook,[28] Google,[29] LinkedIn,[30] LiveJournal,[31] MySpace,[32] Twitter,[33] Zynga,[34] emphasise that they comply with certain American statutes, such as the *Child Online Privacy Protection Act* ('*COPPA*'). As a result of their (stated) compliance with *COPPA*,

---

Cost of Reading Privacy Policies' (2008) 4(3) *I/S A Journal of Law and Policy for the Information Society* 540 <http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf>.

25 Rajen Akalu, 'Implementing PIPEDA: A Review of Internet Privacy Statement and On-line Practices' (10 December 2004) <http://www.priv.gc.ca/resource/cp/2004-2005/p_200405_06_e.asp >.

26 Club Penguin, *Club Penguin Privacy Policy* (11 January 2012) <http://www.clubpenguin.com/privacy.htm>.

27 Blizzard, *Blizzard Entertainment® Online Privacy Policy* (25 March 2011) <http://us.blizzard.com/en-us/company/about/privacy.html>.

28 Facebook, *Facebook Data Use Policy* (8 June 2012) <http://www.facebook.com/full_data_use_policy>.

29 Google, *Google Privacy Policy* (27 July 2012) <http://www.google.ca/intl/en/policies/privacy/>.

30 LinkedIn, *LinkedIn Privacy Policy* (16 June 2011) <http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv>.

31 LiveJournal, *LiveJournal Privacy Policy* (12 December 2010) <http://www.livejournal.com/legal/privacy.bml>.

32 MySpace, *MySpace Privacy Policy* (1 October 2012) <http://www.myspace.com/Help/Privacy>.

33 Twitter, *Twitter Privacy Policy* (17 May 2012) <http://twitter.com/privacy>

34 Zynga, *Zynga Privacy Policy* (30 September 2011) <http://company.zynga.com/privacy/policy>.

these companies avoid knowingly collecting personal information from children under the age of 13, though this does not mean that the companies avoid collecting information *about* children under this age: parents, teachers, and others who interact with young children and youths can and do post public information about such children. The mechanisms that these networks use to avoid collecting PII from children under 13 are often quite crude, amounting to preventing account creation if a person selects an age of less than 13 years. Consequently, a great deal of PII about these children can be, and is, collected on these sites by those who interact with, and share information about, children, as well as by children who are knowledgeable enough to select an age of 13 or older when signing up.

Other companies, including Google, Facebook, LinkedIn, LiveJournal, MySpace, Apple's 'Ping', Twitter, Blizzard,[35] and Zynga, assert their compliance with US-EU Safe Harbour, and some also note compliance with the US-Swiss Safe Harbour Framework. Significantly, between the time of our survey and the time of preparing this paper, MySpace has modified their commitment to US-EU Safe Harbour. Specifically, their policy now reads

> When a Member who is located in the European Union chooses to post Profile Information that will be publicly disclosed, that Member is responsible for ensuring that such information conforms to all local data protection laws. Myspace is not responsible under the EU local data protection laws for Member-posted information.

The conditions that provoked this change remain unknown, though they have occurred as Europe debates their so-called 'Right to be forgotten' principle, which social networking companies have widely opposed.

Foursquare has not adopted the Safe Harbour principles, and explicitly informs its international visitors that,

> 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.[36]

This kind of delegation of responsibility for privacy to users is reflected in a recent statement by Google:

---

35 Blizzard, above n 27.

36 Foursquare, *Foursquare Privacy Policy*, (13 July 2012) <https://foursquare.com/legal/privacy>.

> Responsibility for deleting content published online should lie with the person or entity who published it. Host providers store this information on behalf of the content provider and so have no original right to delete the data. Similarly, search engines index any publicly available information to make it searchable. They too have no direct relationship with the original content.[37]

Moreover, when individuals do have a complaint concerning how one of these services is collecting, retaining, or processing personal data, the companies will often try to restrict where these complaints can be heard. Quite often privacy policies or terms of service will stipulate the jurisdictions and courts through which all legal proceedings must be conducted. Save for Yahoo!,[38] Nexopia,[39] and Plenty of Fish (a Canadian dating social network),[40] which recognise Canadian courts, all claims must go through either American federal or the state courts of California or New York. Only Zynga, a social gaming company, explicitly recognises European jurisdictions, stating that non-US citizens would 'agree to submit to the personal jurisdiction of the courts in Luxembourg.'[41] The full results of which courts these companies recognise are presented in Appendix Two, at least as reflected on the respective homepages accessible in Canada.

In aggregate these findings suggest that there is reluctance on the part of some large social networking companies to declare compliance with European or Canadian data protection laws. Such reluctance may be based on economic incentives, such as wanting to avoid hiring counsel in various nations. Alternatively, large social networking companies know that compliance with data protection laws in the EU and Canada could hinder or forbid practices from which they currently derive commercial benefit. In any event, corporate practices dictate a kind of jurisdiction, insofar as companies assert what they will be held to account for, and where that accounting can take place.

However, they also control the technical infrastructure of these vast data gathering and processing systems. In what follows we discuss how code establishes a different kind of technical 'jurisdiction' by constraining when and where data privacy policies may or may not be enforced.

---

37 Peter Fleischer, 'Our thoughts on the right to be forgotten' on *Google: Europe Blog* (15 February 2012) <http://googlepolicyeurope.blogspot.ca/2012/02/our-thoughts-on-right-to-be-forgotten.html>.

38 Yahoo!, *Yahoo! Privacy Policy* (23 April 2010) <http://info.yahoo.com/privacy/ca/yahoo/>.

39 Nexopia, *Nexopia Privacy Policy* (2 November 2009) <http://www.nexopia.com/privacy>.

40 Plenty of Fish, *Plenty of fish Terms of Use Agreement* (November 2, 2011) <http://www.pof.com/terms.aspx>

41 Zynga above, n 34.

4 Technical 'Jurisdictions': The Networks and their Rules

Scholars have long explored the manners in which technical systems, undergirded by computer coding, often assume a kind of law unto themselves.[42] This characteristic carries over to social networking services, where the coded designs of the platforms can capture, collect, retain, and disseminate users' personal information regardless of formal legal limitations.

Access to personal information requests can reveal something of the magnitude of information that is collected and retained by SNSs. Of the requests submitted under this project, many companies failed to respond, and those that did either refused to provide any information or failed to provide it comprehensively. Of the 11 companies contacted, just six (Facebook, Twitter, Google, Instagram, LinkedIn, or Tumblr) responded in any way.

We begin with Facebook, which now offers 'self-download' features intended for users to access their own information, largely as a result of pressure from the campaign 'Europe v Facebook.' The founder of the campaign, Max Schrems, almost single-handedly exposed Facebook's non-compliance with data protection law and forced the hand of the Irish Data Protection Commissioner, the jurisdiction in Europe where Facebook's corporate HQ are located.[43] The Irish Commissioner's 143-page report into Facebook's data collection and retention principles then led to a major change in Facebook's 'Data Use Policy', including the creation of the self-download feature.[44]

Although the self-download feature does let subscribers access some of the data that Facebook processes, much of the metadata is still being withheld. The most recent inventory, dated April 2012, lists some 57 categories of data obtained by Europe v Facebook in response to a series of access requests, most of which were user-generated. The group also lists a further 27 data elements that had emerged in the course of the complaint to the Irish Data Commissioner. The website also states that there is a further 'internal data set' of additional categories of what can probably be assumed to be 'metadata'.[45]

It is apparent, however, that these categories cannot be precisely defined or distinguished one from another. An earlier network analysis conducted by

---

[42] Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*. (Basic Books, 2006); Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76(3) *Texas Law Review* 553.

[43] Europe v Facebook, *Our Group* (2012) <http://europe-v-facebook.org/FAQ_ENG.pdf>.

[44] Charles Arthur, 'Facebook told to stop indefinitely holding users' advertising data', *The Guardian* (online), 21 December 2011 <http://www.guardian.co.uk/technology/2011/dec/21/facebook-advertising-data?newsfeed=true>.

[45] Europe v Facebook, *Facebook's Data Pool* (2012) <http://europe-v-facebook.org/EN/Data_Pool/data_pool.html>.

Privacy International in 2011 also revealed a more comprehensive listing of data collected by Facebook on its users than the company disclosed through access to information requests.[46] A comparison, however, between the categories of information revealed and not-revealed as a result of these exercises does not yield any meaningful understanding of the scope and type of PII processed by Facebook then and now. The data categories are not equivalent and they have changed over time as Facebook has developed its infrastructure, services, and applications. There is also a clear dilemma about whether the user should be, and can be, provided with personal information that is both meaningful and technically accurate. By repackaging or defining the data pool in order for it to make sense to a non-technical user the company may also be redefining the PII in some significant ways and in effect transforming the data elements themselves.

The dilemma over providing accessible or technically detailed information is revealed when we consider the personal information field made available by Twitter. Twitter's access to information system is heavily reliant on identity authentication. Subscribers to the service first make the request for a full copy of their information. They are then asked to open a ticket with Twitter and then to send the following: a statement authorising the disclosure of the specific information being requested; a statement containing that ticket number; a document with the subscriber's twitter ID; the email address that Twitter has on file as linked to the account; and a scanned copy of government-issued photo identification. After providing this information, Twitter provides a downloadable copy of the user's information. All information contains hashes to ensure that data provided has not been tampered with between the time that Twitter prepares that data and the time when the subscriber downloads that information.

Like Facebook, Twitter provides certain categories of personal information in response to access requests but also withholds a considerable amount of metadata. The following describes the information provided to a subscriber about a single tweet:

> user_id: 14087212
> created_at: Thu Mar 06 06:03:10 +0000 2008
> created_via: web
> status_id: 767404918
> text: Let's learn about Twitter, eh?

The following contains a listing of all the fields and metadata that are actually associated with a tweet circa 2010, which together amounted to 59-60 lines of information: tweet's unique ID; text of a tweet; tweet's creation date; ID of a

[46] Simon Davies, 'Facebook's information access feature still violates European law' on *Privacy International* (22 October 2011) <https://www.privacyinternational.org/blog/facebooks-information-access-feature-still-violates-european-law>.

tweet that is being replied to; screen name and ID of who is being replied to; whether the tweet has been favourited; whether the tweet has been truncated to 140 characters; the author's user ID; the author's user name; the author's screen name; the author's biography; the author's URL; the author's location; rendering information of the tweet; the creation date of the account; whether the account has contributions enabled; number of tweets the user has favourited; number of users the author is following; the user's time-zone and time offset; number of tweets the user has; the user's selected language; whether the user's account is set to protected status or not; number of users following the author's account; whether the user has geo-locational tagging enabled; place IDs; the user's contribution ID, if they have one; URL to fetch a detailed polygon for the place location; printable names of the place; the place associated with the tweet; type of place (eg neighborhood or city); country the place is in; bounding CSS for the place; and the application that sent the tweet.[47] It is in light of Twitter's reluctance to provide full metadata information that one Canadian citizen has filed a formal complaint to the Office of the Privacy Commissioner of Canada; the case remains unresolved.[48]

Google also monitors its users' actions as they move across the company's services. In response to access to personal information requests, the company failed to include IP addresses, locational information (where appropriate), and a range of other data.[49] It is striking that when we filed an access request to Apple, to learn what data their 'Ping' service collected, we found that the company was entirely unable to provide information related to the service, despite the system being in operation at the time of the request. Only customer service relations information pertaining to Apple hardware (eg MacBook, Apple Time Capsule router) warranty claims were disclosed; even transactions for applications on Apple's online markets were excluded from Apple's responses.

The failure fully to disclose subscribers' information matters because apparently minor items may have significant consequences, especially when seen in combination with other data fields. What is normally being excluded through the download or access tools tend to be metadata, which can reveal geo-locational information, information about social networks, and broader communications patterns that are not evidenced in a single statement, tweet, or Facebook message. Metadata can reveal the activity of a user on any

---

47 To see this information in visual format, see: Christopher Parsons, 'Twitter, Mobile Browsers, and Metadata Privacy' on *Technology, Thoughts, and Trinkets* (22 April 2010) <http://www.christopher-parsons.com/blog/technology/twitter-mobile-browsers-and-metadata-privacy/>.

48 Based on personal correspondence between Christopher Parsons and the complainant.

49 To date, no full traffic analysis of Google metadata has been performed. Doing so would require performing a man-in-the-middle attack to decrypt data transmitted between Google and a client computer, and is presently outside the scope of our research project.

specific social network and times of activity, as well as relative affluence based on devices used to communicate with the social network, and technical sophistication based on the client software that is used. It can also be used in conjunction with other users' metadata for commercial data mining purposes. So, the non-disclosure of this information is significant insofar as the power to write the download tool itself empowers particular corporate agents to judge what is personal, what is not, and often what information *can* be granularly extracted from these systems as relating to specific and identifiable individuals. The decisions to make information 'accessible' to end users, in effect, has significant implications for the ability to understand the information provided to social networks, information that is subsequently used for service delivery and commercialisation.

So, while we can gain some insight by actually testing the download options provided by some networks, we can also learn about how technical systems affect the companies' own policies. Google, as an example, recognises that even after deleting account information, it may persist, indefinitely, on backup systems.[50] Facebook's deletion process has raised similar questions in the past,[51] and Tumblr notes that their systems cannot delete users' 'public activity.'[52] Similar assertions are issued by Foursquare.[53] Other companies' policies, such as Nexopia and Meetup, assert that subscriber data can never truly be removed from databases. We have argued elsewhere that these practices constitute a process of 'quasi-forgetting.'[54]

The only other companies that replied to our requests for our personal information were LinkedIn, Instagram, and Tumblr. Both LinkedIn and Instagram engaged researchers in discussion — LinkedIn opened a ticket, but failed to provide researchers with the full range of personal information that they had collected, used, or processed about them. Instagram responded with some basic account information in an email attachment that included the following: a user ID number; username; first name; last name; email address; gender; birthday; phone number; biography; a user entered website address;

---

50 Google, 'Our thoughts on the Right to be Forgotten' on *Google Europe Blog* (16 February 2012) <http://googlepolicyeurope.blogspot.ca/2012/02/our-thoughts-on-right-to-be-forgotten.html>.

51 Jacqui Cheng, 'Three years later, deleting your photos on Facebook now actually works' on *Ars Technica*, (16 August 2012) <http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting/>.

52 Tumblr, *Privacy Policy* (22 March 2012) <http://www.tumblr.com/policy/en/privacy>.

53 Foursquare, above n 36.

54 Colin J Bennett, C J Adam Molnar and Christopher A Parsons, 'Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice' (2013) *Social Science Research Network* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208098>.

an indication of whether the account is private/public; whether the account is 'active'; date user joined the service; signup IP address; all user relationships, incoming requests, and followers, and whether these accounts are themselves public or private; and all user published media during the date range that the account has been active. Interestingly, an identifier at the top of the file reads '[username]_subpoena_01/15/13', indicating a potential match with that shared with authorities under lawful access, and specifically under subpoena, circumstances. The data from Instagram was received after a prolonged period of negotiation with the company, who saw it as economically and technically impractical to deliver a full accounting of the information that it possessed about the requester. As such, the information received was a template of the data stored by Instagram, as opposed to a comprehensive record of the information retained by the company on the user in question.

In the case of Tumblr, the company's legal staff stated that the company,

> will not be providing the information you requested. Tumblr is a US-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.'[55] The stated requirement to work through New York courts is interesting, given that Tumblr's privacy policy only recognises 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.

In addition to these difficulties in requesting access to their personal data, subscribers to these services also face challenges in communicating their concerns about how the company may be 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. That said, two services, LiveJournal and MySpace, recognise 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

[55] Michael Sussmann, Personal e-mail with Christopher Parsons.

though, in subsequent research, we found that its staff did at least engage the researchers in discussions about their requests for user data.

Hence, it can be incredibly challenging to access one's personal data, save for the limited disclosures of information provided by the three largest companies, Facebook, Twitter, and Google. Moreover, even when data has been provided it has been limited and, arguably, not comprehensive on the basis that the metadata associated with social networking communications are not provided. Finally, even trying to complain about the services — or contacting a privacy officer to learn about how personal information is captured and can be downloaded by the subscriber — is challenging given the relative absence of effective complaints mechanisms. It appears that citizens can *only* comprehensively learn what information the companies have been collecting if they involve a national regulator, a task for which few citizens would have the resources or inclination. These results are predictable. They are also ironic, given that the raison d'etre of social networking is to promote the relatively frictionless sharing of personal information and to facilitate engagement of personal conversations between individuals.

5 Conclusion

The full implementation of the range of privacy protection rules within social networking environments is governed by both legal interpretation and corporate policy. More importantly, it is governed by the ways in which the collection and processing, and even definition, of personal data, is instantiated by the way that computer code is designed. There are then three sets of rules (legal, corporate and technical) that operate on different jurisdictional dimensions.

For any privacy protection law to be seriously implemented in a social-networking environment, these three dimensions must be in alignment. They rarely are. The formalities of legal jurisdictions and the abstract disputes over whose laws apply when and where tend to operate on a different plane from the worlds of corporate policy and technical infrastructure development. Moreover, as our attempts to assert our access to personal information rights reveal, the corporate policy dimension only imperfectly interacts with the technical in the best of cases. The law says that compliance should flow from a 'real and substantial connection' to Canada. The case studies demonstrate that Canadian legal rules, and we would assume other law as well, confront a set of corporate and technical 'rules' that can be extraordinarily difficult to shift.

Non-compliance is not necessarily the result of corporate actors deliberately, consciously, or cynically deciding that some laws do not merit compliance. Our findings suggest that non-compliance is a more structural phenomenon, one that is institutionalised by the disjunctures between three related, but separate, systems of rules. These systems, and the associated forms of jurisdiction, flow almost independently and they only interact in better alignment when there are extraordinary outside interventions.

Regulatory investigations by privacy and data protection authorities can be one such intervention. One broad lesson for regulators, therefore, is that their compliance investigations can force real change, particularly when there is cross-jurisdictional enforcement, as is contemplated under the enforcement regime within the new EU Draft Regulation[56] and within the new Global Privacy Enforcement Network. Our research indicates that such cooperation and the 'joined up' governance for privacy and data protection can expand the prospective influence of regulators.[57] It also indicates that the kinds of corporate accountability mechanisms (codes of conduct, privacy impact assessments, binding corporate rules), as well as the technological instruments (privacy by design and by default) need closer integration into systems of legal compliance.

For the broader network of privacy advocates, and as documented in Bennett's prior work,[58] there can be mileage in well-conceived and articulated complaints to data protection authorities. Despite the skepticism about the utility of official data protection commissioners in some quarters of the privacy advocacy community, the well-targeted complaint aimed at the appropriate regulator remains a useful instrument in the toolbox of the contemporary privacy activist. Personal information access requests, on the other hand, can be frustrating and revealing of nothing more than corporate intransigence and/or incompetence. Such requests also need to be targeted and framed appropriately because in some jurisdictions they can be discounted if perceived as a 'research exercise' rather than a 'genuine' exercise of rights. Nevertheless, if we are correct in observing a trend towards off-loading compliance with data protection law to the user, then the modest efforts by Facebook, Google, and Twitter to recognise consumer rights of access may be indicative of future trends.

For researchers, there is clearly potential to replicate this study with respect to the top SNSs in other countries. What is the public profile of the SNS in other jurisdictions? Are Europeans, Australians, Japanese, and others told the same as Canadians about their rights? How would compliance be affected by the significant presence of localised SNSs in some countries; such as Mixi in Japan, Cyworld in Korea, iBiBo in India, Renren, Douban Kaixin001 and Qzone in China and Nasza-Klasa/nk in Poland? And how would the dominant social networks respond to the assertion of access to personal information rights in different jurisdictions?

---

[56] *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), opened for signature 25 January 2012 [2012] <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.

[57] An example of this prospective cooperation is the Global Privacy Enforcement Network (12 April 2012) <www.privacyenforcement.net>.

[58] Colin J Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, 2009).

We suspect that a systematic comparative analysis along the lines offered here would not only be valuable for advocates and regulators but would also expose the contradictions, incoherencies and inconsistencies to the social networks themselves. If nothing else, this survey has demonstrated that social networks are not on the same page with respect to compliance. Despite the prolific collection and sharing of subscribers' personal information, these companies do not seem to have shared common best practices about compliance with privacy or data protection laws.

Appendices

Appendix 1: Does the SNS say it complies with any national privacy laws, international guidelines or self-regulatory mechanisms (ie a 'good housekeeping' seal of approval, such as TRUSTe)?

SNS	LAWS/GUIDELINES	DISPLAY OF PRIVACY SEAL
Blogger (Google)	Yes: US-EU Safe Harbour Framework; US-Swiss Safe Harbour Framework; UK Internet Advertising Bureau Good Practice Principles for Online Behavioural Advertising; Australian Best Practice Guideline for Online Behavioural Advertising; IAB European Framework for Online Behavioural Advertising; member of Network Advertising Initiative.	No
Club Penguin	Yes: US Children's Online Privacy Protection Act; EU Data Protection legislation; Canadian federal and provincial legislation; all applicable privacy laws relating to provision of financial services; Safe Harbour Principles (when using or disclosing PII transferred from the EU, Switzerland or Australia to the US).	Yes: TRUSTe Children's Online Privacy Seal Program
Facebook	Yes: California law; US-EU and US-Swiss Safe Harbour Frameworks.	Yes: TRUSTe EU Safe Harbour
Flickr (Yahoo)	No	No
Foursquare	Yes: compliance with 'applicable laws' of US and state governments, law enforcement and regulatory agencies.	No
Google +	See Blogger (Google)	
Instagram	No	No
LinkedIn	Yes: EU Safe Harbour Privacy Framework, as administered by the US Department of Commerce; self-certification of compliance with US-EU Safe Harbour Principles; member of Council of American Survey Research Organizations and abides by their guidelines for market research.	Yes: TRUSTe Privacy Seal

LiveJournal	Yes: US Department of Commerce's Safe Harbour Program; Council of Better Business Bureaus, Inc. EU Safe Harbour 'independent dispute resolution mechanism.'	No
Meetup	No	No
MySpace	Yes: US-EU and US-Swiss Safe Harbour Frameworks, as set forth by US Department of Commerce; adheres to Safe Harbour Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement; committed to BBB EU Safe Harbour 'dispute resolution mechanism.'	No
Nexopia	No	No
Ping (Apple)	Safe Harbour frameworks set forth by the US Department of Commerce regarding collection, use and retention of PI collected by organisations in the European Economic Area and Switzerland.	No
Pinterest	No: mentions only that 'Pinterest cooperates with government and law enforcement officials.'	No
Plenty of Fish	No: references 'applicable privacy laws.'	Mo
Reddit	No	No
Tumblr	Yes: California Civil Code, sections 1798.83-1798.84 (California residents are entitled to ask for a notice identifying the categories of personal customer information shared with affiliates and/or third parties.	No
Twitter	US-EU and US-Swiss Safe Harbour Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement.	No
Wikimedia Foundation	No	No
WordPress.com	No	No
WordPress.org	No	No

World of Warcraft	Yes: US-EU and US-Swiss Safe Harbour Frameworks, as set forth by the US Department of Commerce regarding collection, use and retention of personal information from EU member countries and Switzerland; self-certification of adherence to Safe Harbour Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement; California law (residents may request certain information regarding disclosure of personal information.	Yes: TRUSTe Privacy Seal
YouTube (Google)	See Blogger (Google)	See Blogger (Google)
Zynga	Yes: US-EU and US-Swiss Safe Harbour Frameworks, as set forth by the US Department of Commerce regarding collection, use and retention of personal information from EU member countries and Switzerland; self-certification of adherence to Safe Harbour Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement; references California Privacy Rights.	Yes: TRUSTe Privacy Seal

Note: Research findings are as of 29 July 2012.

Appendix 2: Does the SNS specify any nations or courts through which legal proceedings must occur?

SNS	JURISDICTION
Blogger (Google)	Terms of Service (ToS) states that all claims will be litigated exclusively in the federal or state courts in Santa Clara County, California.
Club Penguin	ToS states that all claims shall be filed in courts located in the borough of Manhattan, City of New York, State of New York, United States of America.
Facebook	ToS states that all claims will be resolved in a state or federal court located in Santa Clara County, California.
Flickr (Yahoo)	ToS states that 'you and Yahoo! agree to submit to the personal and exclusive jurisdiction of the courts located within the province of Ontario.'
Foursquare	ToS states that 'parties consent to exclusive jurisdiction and venue in the United States Federal Courts or state courts located in the Southern District of New York.'
Google +	See Blogger (Google)
Instagram	No
LinkedIn	ToS states that 'you and LinkedIn agree to submit to the personal jurisdiction of the courts located within Santa Clara County, California… Notwithstanding the above, you agree that LinkedIn shall still be allowed to apply for injunctive remedies (or an equivalent type of urgent legal relief) in any jurisdiction.'
LiveJournal	ToS states that 'you and LiveJournal agree to submit to the personal and exclusive jurisdiction of the courts located within the county of San Francisco, California, U.S.A.'
Meetup	ToS states 'you and Meetup agree to submit to the personal and exclusive jurisdiction of the courts located within the State of New York.'
MySpace	ToS states 'you and Myspace agree to submit to the exclusive jurisdiction of the courts located within the State of New York.'
Nexopia	ToS states 'you agree to submit to the exclusive jurisdiction of the courts of the Province of Alberta and the Federal Courts located within the Province of Alberta.'
Ping (Apple)	ToS states 'you agree to the personal jurisdiction by and venue in the state and federal courts in Santa Clara Country, California.'
Pinterest	ToS states 'we each agree to submit to the personal jurisdiction of a state court located in Santa Clara County, California or the United States District Court for the Northern District of California.'

Plenty of Fish	ToS states 'as a condition of using the Services, each user agrees that any and all disputes and causes of action arising out of or connected with Plentyoffish shall be resolved through arbitration, with such arbitration to be held in Vancouver, British Columbia, Canada.'
Reddit	User agreement states that both parties agree to submit to the exclusive personal jurisdiction and venue of the state or federal courts in New York.
Tumblr	ToS states 'you agree to submit to the personal jurisdiction of the courts located within New York County, New York.'
Twitter	ToS states 'all claims […] will be brought solely in the federal or state courts located in San Francisco County, California, United States.'
Wikimedia Foundation	ToS states 'if you seek to file a legal claim against us, you agree to file and resolve it exclusively in a state or federal court located in San Francisco County, California.'
WordPress.com WordPress.org	ToS states: 'any dispute arising under this Agreement shall be finally settled in accordance with the Comprehensive Arbitration Rules of the Judicial Arbitration and Mediation Service, Inc. ('JAMS') by three arbitrators appointed in accordance with such Rules. The arbitration shall take place in San Francisco, California, in the English language and the arbitral decision may be enforced in any court.'
World of Warcraft	No
YouTube (Google)	End User Licence Agreement states 'if you are a resident of the United States, any arbitration will take place at any reasonable location convenient for you. For residents outside the United States, any arbitration shall be initiated in the County of Los Angeles, State of California, United States of America.' See Blogger (Google)
Zynga	ToS states 'if you are a resident of the United States [...] you agree to submit to the personal jurisdiction of the courts located within San Francisco County, California […] If you reside outside of the United States […] You agree to submit to the personal jurisdiction of the courts in Luxembourg.'

Note: Research findings are as of 29 July 2012.