# If these Canadians lived in the United States, how would they protect their privacy?

Colin J. Bennett, Priscilla M. Regan, and Robin M. Bayley

March 2017

First Monday, Volume 22, Number 3 - 6 March 2017

PEER-REVIEWED JOURNAL ON THE INTERNET

# If these Canadians lived in the United States, how would they protect their privacy?

by Colin J. Bennett, Priscilla M. Regan, and Robin M. Bayley

## Abstract

This paper contributes to the debate about the adequacy of the United States' fragmented, networked, federal system of privacy protection, an outlier among modern industrialized Western democracies, by taking the perspective of an individual seeking redress for privacy invasions. We analyze five actual privacy cases from the Canadian private sector, investigated by the Privacy Commissioner of Canada, and examine whether the privacy "wrong" experienced by Canadian complainants would be illegal in the U.S., how an individual would proceed with a complaint and what the outcome might be. We attempt therefore to bring the debate away from the typically abstract institutional and legal approach to the level of the regime's practical effectiveness. Despite well-documented flaws in the Canadian privacy protection system, from the point of view of the average citizen, it provides a more consistent, transparent, accessible and effective means for making privacy complaints and having them investigated and resolved, especially when the personal data is captured online.

**Contents**



## Introduction

The United States has never passed a comprehensive privacy protection (data protection) statute, nor established a single privacy (data protection) commissioner, as exist in Europe, Canada and most other democratic countries. Some argue, however, that the sum total of all federal and state, statutory, tort and constitutional law constitutes an overall privacy regime that offers much the same combination of individual rights and organizational obligations as exists elsewhere. Defenders of the U.S. approach point out that privacy, and the doctrine of fair information principles, has deep roots in American cultural and historical traditions (Westin, 1967; U.S. Department of Health, Education & Welfare (DHEW), 1973). A "networked and layered" approach to protecting personal information has evolved organically, consistent with the separation of powers, the Bill of Rights and American federalism (Kropf, 2007). This approach is different from that in other countries, but it is "essentially equivalent" (Sidley Austin LLP, 2016).

Critics see the system differently. American privacy protection was "fragmented, incomplete and discontinuous" (Gellman, 1993), and "remains fragmented and ambiguous, siloed and sectoral" [1]. There are some huge gaps in coverage, including the vast majority of business to consumer (B2C) services provided online. Reidenberg (2013) contends that the European approach puts citizens first, corrects market biases, incentivizes good business practice and provides redress and independent oversight. In Europe and other advanced democratic countries, citizens and individuals know whom to contact if they experience a violation of their privacy rights — the independent data protection agency (DPA). For all the "networked and layered oversight" in the U.S., the American consumer has no such clarity of recourse.

Comparisons between the U.S. privacy regime and the data protection systems in Europe have invariably been made in the context of rhetoric about transatlantic "data wars" (Regan, 2003, 1993; Farrell and Newman, 2016) and highly politicized justifications of one system over another (U.S. Mission to the European Union, 2013). The rhetoric has only reached new levels of stridency after the Snowden revelations and the ongoing dispute between EU and U.S. policy-makers about the demise of the Safe Harbor Agreement, and about its replacement (the 'Privacy Shield'). It is probable, as Kuner (2014) remarks, that "neither the EU nor the U.S. properly understands each other's approach to data privacy."

We contend that blanket and national comparisons between privacy regimes are often misleading. Privacy protection

law is simply not amenable to objective standards of measurement according to analysis of the 'black letter of the law.' Claims about adequate or equivalent 'levels' of protection obscure the multi-faceted nature of privacy rights and obligations, and generally overlook essential, but more subjective, understandings about political and administrative cultures and traditions. As Bennett and Raab (2006) have argued, "Data protection should be seen not just as a system that produces outputs and outcomes, but as a process that involves organizational change and learning, and that involves an elaborate implementation network of persons and organizations engaged in the collaborative, albeit often conflictual, production of data protection." [2]

In this paper we adopt a new approach to the evaluation of U.S. privacy protection policy. While we agree that a comparative approach and yardstick is necessary, we also believe that evaluation to an undifferentiated "European" privacy regime is inherently misguided and that the Canadian system is a more equivalent point of comparison. Similar to the U.S., Canadian privacy law evolved pragmatically according to its distinctive federal, constitutional framework. But at a critical point in the 1990s, the Canadian government decided, for a variety of domestic and international reasons, to follow the European lead and enact a comprehensive privacy statute for the private sector and to give oversight responsibility to the Office of the Privacy Commissioner of Canada (OPC). The system of privacy protection under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), now in its seventeenth year of operation, provides a valuable reference point for private sector privacy enforcement in the U.S.

We also contend that effective evaluation requires the disaggregation of the elements of the privacy protection model. Any one privacy regime provides a complex array of privacy rights and organizational obligations. Each expects organizations to take preventive measures, and also provides after-the-fact remedies when violations occur. For the purposes of this analysis, we concentrate on just one essential component of any privacy protection regime: the ability to provide redress for individual complaints and grievances, a function that is at the heart of any privacy protection policy. The ability to provide "support and help to data subjects in the exercise of their rights" rapidly, effectively and without prohibitive cost has been an essential condition for the assessment of an "adequate data protection" for the transfer of personal data outside the EU under the 1995 Data Protection Directive (European Commission, Article 29 Working Party, 1998).

Therefore, we go beyond comparing legal rules in the abstract, and assess effectiveness in terms of the ability of the privacy regime to give assistance and redress to real individuals who have suffered privacy harms. We take a sample of Canadian cases of individuals who have registered complaints at the OPC about companies under PIPEDA, and then ask the question: "if these individuals lived in the United States, what would be the process of complaint and redress under American law?" Hence, we try to draw comparisons by looking at the experiences of real individuals who have claimed a breach of their privacy, and who have successfully found redress through the Canadian system.

We first outline the process of individual complaints resolution under PIPEDA, noting that the Canadian system has been subject to a good deal of criticism itself. We then justify our choice of cases investigated and resolved in the areas of: online advertising; online dating; data breaches in insurance; hotel registration systems; and cellular telephone services. For each case, we then ask: if these same fact situations occurred in the U.S., to which federal and/or state institutions could the individual bring his/her case, and under which legal instrument? Although we compare only one significant aspect of a successful privacy protection regime, that of redress, this article offers an insightful comparison of the two systems from the point of view of the average consumer, and we hope it presents lessons for both American and Canadian policy-makers. We are not aware of any research in the privacy literature that has adopted a similar approach.

## The complaints process under PIPEDA

PIPEDA (dating from 2000) is Canada's national privacy law governing the federally regulated sectors such as interprovincial transportation and shipping, banking, telecommunications and broadcasting, as well as to the commercial activities of organizations that transfer personal data for commercial purposes across provincial and international borders. It also applies to the activities of commercial organizations in provinces and territories that do not have their own private sector privacy statutes — that is, everywhere except British Columbia, Alberta and Quebec. While the law mainly applies to Canadian organizations, it also covers the personal information practices of foreign organizations that capture, store, use and disclose personal data within Canada, or where there is a "real and substantial connection" to Canada.

PIPEDA is based on 10 familiar fair information practices, contained in the Canadian Standards Association's (CSA) *Model code for the protection of personal information* (CSA, 1996) [3]. Enforcement is primarily complaint-driven, but the Privacy Commissioner also has proactive powers to investigate on his or her initiative, to educate the public, to publish research and to promote compliance programs. The Commissioner is an independent officer of Parliament, selected by an all-party committee. He or she has no order-making powers, but is an ombudsman who tries to resolve disputes through negotiation, mediation, conciliation and, if necessary, the threat of publicity. The model is a common form of regulation in Canada, but somewhat unique in its application to private sector organizations (Perrin, *et al.*, 2001). One of the main strengths of PIPEDA enforcement is that the threshold for filing a complaint is low. Individuals who allege a transgression of the law may lodge a complaint without cost, legal representation or having to prove harm. The OPC expects complainants to try to resolve the issue with the organization before filing a complaint. It also publishes helpful tips for the individual and supports an electronic filing process [4].

After ensuring that the OPC has jurisdiction, it attempts informal resolution where possible but may proceed to a formal investigation. Investigators have delegated power to receive evidence, enter premises and compel the production of records. The Investigator sets out the facts and makes recommendations, and may allow further representations. He or she will consult internally and forward recommendations to the Privacy Commissioner or his delegate, who issues a confidential preliminary report. The organization can respond to an adverse decision with a plan to remedy the matter.

There are three potential final outcomes of an investigation: well-founded (the Commissioner upholds the complaint); well-founded and conditionally or actually resolved (the organization has made changes, or committed to making changes, to make itself compliant); and not well-founded (finding in favor of the organization) (OPC, 2015b). If an investigation results in a "well-founded" decision against the organization and it does not undertake to make recommended changes to its personal information practices, the Commissioner can enforce his or her finding by applying to the Federal Court, which may then issue a binding decision and award damages, if appropriate.

Recently passed amendments to PIPEDA allow the Commissioner to enter into a compliance agreement with the organization, in which the organization agrees to take certain steps to bring itself into compliance, and which precludes the Commissioner from commencing any court action (OPC, 2015a). But, as an ombudsman, the Commissioner has no independent enforcement powers to levy fines, award damages or order the organization to change its practices, something the current Commissioner, Daniel Therrien, has asked Parliament to reform (Schmitz, 2016).

The pros and cons of the ombudsman model have been the subject of a number of studies (*e.g.*, Houle and Sossin, 2010). Some have suggested that the OPC, as an ombudsman organization, may be more concerned with what is realistic — what it can get the organization to willingly agree to — than what is ideal. Sometimes, its interest in a long-term relationship with a powerful company may lead the OPC to settle for solutions that the individual would not accept and which may fall short of a strict application of the law (Berzins, 2010). Further its recommendations are of less value as precedents, than if they were binding enforcement orders.

Another drawback is that the OPC is statutorily restricted in its ability to disclose information gained in the exercise of his or her duties. Case summaries typically name neither the organization nor the individual, and are often short on detail. The consequences for an organization's reputation are not as serious as if they were named, and defending a privacy complaint may be less of a deterrent to "pushing the envelope" with questionable privacy practices (Geist, 2012).

The vast majority of cases do not result in case summaries. In 2014, of 375 cases closed by the OPC, 187 were resolved or settled early, 49 were withdrawn (often because they dealt with issues whose outcome was very clear, based on previous cases), and in 68 cases the OPC either declined to investigate or had no jurisdiction. That left only 58 of 375, or 15 percent, of cases, which went through the whole investigation process and resulted in a finding. As an illustration of the pattern, in 2014, 43 percent of findings were deemed not well-founded and 57 percent were well-founded in some respects (OPC, 2015b).

The OPC complaint process can also be quite lengthy. The cases resulting in findings took from 12 to 27 months, on average, in contrast to early-resolution cases taking 2.4 months. Those statistics may discourage individuals hoping for speedy resolution or for an interpretation — a "lesson learned" — that can benefit the public. The complaints process has also been criticized for its lack of communication with complainants, allowing little or no input or influence after filing (Berzins, 2010). Complainants are not guaranteed an opportunity to respond to the organization's response to the complaint, to supply additional evidence or to contest an organization's assertions.

Despite the noted shortcomings, the law does establish a baseline standard of fair information practices across the private sector, and there have been some notable, and internationally renowned, successes (particularly against large multinational companies like Google and Facebook). The OPC has also issued helpful guidance across a range of privacy issues. There is evidence of a growing awareness of privacy issues within Canadian businesses, and that an increasing number have procedures in place to address privacy risks (Phoenix Strategic Perspectives, 2016). It is also the case that many individuals have successfully used PIPEDA to protect their privacy rights. We now analyze a selection of these individual cases.

## Methodology and case selection

Although we have not selected a representative sample of cases, we have attempted to choose cases systematically and according to some reasonably strict criteria.

First, the organizations that were investigated by the OPC obviously need equivalents in the United States; interestingly but not surprisingly, in some cases the organizations investigated by the OPC are in fact U.S. companies whose personal information practices affect Canadians.

Second, we have also tried to find cases across a range of sectors, so that the effectiveness of different U.S. sectoral laws can be examined. Each of the cases has an Internet component as very few organizations, if any, operate entirely off-line. So all our cases have an online component, even if as basic as the transparency and completeness of the online privacy notice.

Third, we have excluded cases involving relatively mundane procedural issues, preferring to concentrate on issues with substantive privacy questions. The selected cases illustrate a wide range of information privacy questions on collection, use, retention and disclosure and concerning issues concerning consent, subject access rights, correction, security and data breaches.

Fourth, we have chosen cases where at least some of the complainant's argument was accepted by the OPC, and where also, crucially, the company responded with changes to its practices and/or the OPC was able to issue guidance about the meaning of the law. Thus, we have picked cases where the system has, at least partially, 'worked' for the complainant, where redress has been achieved, and where the organization has responded positively and changed its practices accordingly.

Fifth, we also assume that the initial attempts to resolve the complaint without intervention from the OPC were not successful. In both Canada and the U.S., many privacy issues may be successfully resolved in confidence, without

recourse to the oversight body. We want to find what a complainant might do under the law, and not under company policy or an industry association code of conduct.

Sixth, we have excluded cases under the jurisdiction of provincial legislation, focusing entirely on one Canadian law (PIPEDA), and one supervisory authority (OPC). The research is driven by the facts of the Canadian case, but in the United States those facts might open up possible avenues of redress at both federal and state levels.

Finally, there are a handful of cases where the OPC has collaborated with the U.S. Federal Trade Commission (FTC) on the investigation and resolution of privacy cases. Both the OPC and the FTC now collaborate in the Global Privacy Enforcement Network (GPEN), designed to increase cross-national collaboration in privacy enforcement (Bennett, 2015). We have excluded any joint investigations from consideration, as we are interested in the comparison of distinct and separate processes on each side of the border.

The facts and results of privacy investigations under PIPEDA are summarized on the OPC's Web site, but the record is not comprehensive and the reporting of the case materials is inconsistent. We have, therefore, had to look in a range of around 10 years to find a selection of cases that fit our criteria. For the most part, the identity of the company under investigation is not revealed in the summaries, with one exception (Google).

**Five Canadian privacy cases and the legal options for redress in the United States**

In describing the Canadian cases here, we briefly describe the facts, outline the privacy principle(s) that complainants allege that the organization has contravened, define what transpired during the investigation and report the result or finding. Next, we turn to the U.S. to examine what forms of redress would be available to the individual under the same factual situation. We answer this question as though we were the individual seeking redress — not as though we were a lawyer acting for the individual. We attempt to find the various paths that an individual would likely find if he or she had a privacy issue similar to that in each of the Canadian cases, and then to assess the likely response that the individual would receive if he or she pursued each path that seemed available.

*Case One: Google allows sensitive personal health information to be used to target ads, without consent*

The complainant [5] alleged that, since he had searched online for medical devices for sleep apnea [specifically, a Continuous Positive Airway Pressure (CPAP) device that is used during sleep], various Web sites that display advertisements from Google's AdSense service often served him advertisements for CPAP devices while he was on unrelated sites. The complainant viewed his browsing and search history relating to sleep apnea as sensitive personal information that should not be used for targeted advertisements without his express consent.

Principle 4.3 of PIPEDA states that the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate. Principle 4.3.6 stipulates that the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive.

The OPC investigated and tested the complex technical workings of the Google advertising system. Google argued that it had policies requiring all advertisers using a "remarketing" platform to avoid all forms of interest-based advertising involving sensitive categories, including the use of user lists based on "health or medical information." As such, they argued that it was the remarketer's error, not Google's. It also argued that it had monitoring systems in place, but the OPC determined that there were shortcomings and, in this instance, the system had not worked. In its Preliminary Report, the OPC recommended that Google ensure that no sensitive information be used to deliver advertisements without express consent.

In response, Google proposed certain remedial and technical measures, and removed all active remarketing campaigns involving CPAP devices. It committed to revising its public interest-based advertising policies and developed new training for staff. It increased monitoring of existing remarketing campaigns, and committed to reviewing and upgrading its automated review systems. To date, the allegation was *well-founded and has been conditionally resolved*.

Turning to the U.S., an individual would have no legal right to restrict the flow of his browsing history, even if browsing involved medical conditions or other sensitive personal interests. A 2015 study by Libert analyzed third-party tracking of Americans' visits to Web sites while seeking health-related information and found that Google was "the gorilla in the room," although by no means the only large entity in that room. He found that 78 percent of the pages analyzed included elements owned by Google, which "means that a single company has the ability to record the web activity of a huge number of individuals seeking sensitive health-related information without their consent" [6]. In this instance the American would be in a similar situation to the pre-complaint Canadian with respect to Google — but with fewer options to redress his grievances.

The *Health Insurance Portability and Accountability Act of 1996* (HIPAA) does not regulate or oversee business practices by third party commercial entities or data brokers. Nor is it likely that the FTC's Health Breach Notification Rule would apply since the information was not lost or stolen. Instead, the primary "regulation" in this area of behavioral advertising is self-regulation by Google and the online advertising community. The Network Advertising Initiative (NAI) does have a Code of Conduct requiring consumer consent for advertisers to use specific information about certain serious health conditions [7]. Similarly, the Digital Advertising Alliance (DAA) has rules that provide minimal protection for health information, but these rules do not prohibit tracking online searches for general medical conditions [8].

Regarding the specific issue of remarketing, Google's defense in the Canadian case, it is important to reiterate that in the U.S. no law prohibits an advertiser from placing targeted ads based on an individual's previous online activity. If the Web site indicates that it adheres to certain guidelines, for example those of the NAI or DAA, and if an individual believes that he or she has received ad content based on sensitive health information, this may constitute a deceptive

practice and the individual may be able to file a complaint with the FTC. If Congress were to pass "do not track" legislation, as the FTC and privacy groups have recommended and has been proposed for several years, then such targeted advertising would be regulated (CDT, 2009; U.S. Federal Trade Commission (FTC), 2010).

The individual may also find that some state consumer protection laws apply in this situation and find a sympathetic ear at a state Attorney General (AG) office. As Citron (2016) reports, state AGs have become more active in the privacy arena and may indeed be inclined to investigate a complaint along these lines. In 2002, 10 state AGs, led by New York, reached a settlement with DoubleClick about its online advertising practices in which it agreed to develop a tool to help consumers track how ads are served to them (Miles, 2002).

*Case Two: Online dating service commits multiple privacy infractions*

A member of an online dating service canceled his membership and asked for his personal information to be deleted and that he be removed from the organization's mailing lists [9]. He also sought access to his personal information held by the organization. Yet, he continued to receive email communications, was denied his personal information and was told it was not in the database. During the OPC investigation, the organization insisted it had purged the personal information.

The OPC found that the organization: denied the complainant access to his personal information, in violation of Principle 4.9 of Schedule 1 of PIPEDA; failed to respect the 30-day time limit for providing access to an individual's personal information under subsection 8(3); failed to safeguard the complainant's personal information against unauthorized use, as required by Principle 4.7.1; retained the complainant's information after it was no longer required to deliver dating services, after withdrawal of consent, in contravention of Principle 4.5.3; initially had no privacy policy in place, in contravention of Principle 4.1.4(d); and destroyed the photographs, limiting the complainant's ability to exhaust all recourse regarding his access request. In all respects, the complaint was *well-founded and resolved*.

The personal information handling practices of online dating sites in the U.S. are not subject to any federal law. Thus practices will vary by site, as will the stated commitments in any company privacy notice. If the site does not follow its stated practice or changes its policy without warning, the first recourse will be to deal directly with the Web site, to request to have information and photos deleted and to cancel the account.

According to the Privacy Rights Clearinghouse (2012), even if one cancels an account with a dating site, the site generally will retain that information — in case the individual wants to return. The Electronic Frontier Foundation (EFF) points to two problems which may result from the retention of information by dating sites: first, it would be available to others (law enforcement, private investigators or divorce lawyers, for example); and second, photos, even those once deleted, are not held by the dating site but by a content delivery service (Reitman, 2012).

If an individual is not satisfied dealing with the dating site, then he or she could take a complaint to the FTC, which again will be looking for patterns of unfair or deceptive practices, assuming the site has publicized a privacy policy. Although there is no federal law regulating online dating sites, a handful of states have laws regulating either or both privacy and safety on online dating sites, but in most cases these are simply 'consumer beware' laws, and only involve requiring or suggesting that the site have a privacy policy or privacy practices in their terms of service [10].

If there is no state law, individuals with grievances about the information practices of online dating sites could work through their state's AG's office. Interestingly, California's AG signed an agreement with three of the largest online dating sites (eHarmony, Match.com and Spark Networks) in 2012 to establish common policies and consumer protections regarding identity theft, financial scams and sexual predators, but did not address privacy practices [11].

*Case Three: Insurance company overhauls its security safeguards following privacy breach*

The complainant claimed that the respondent lost the personal information in his insurance file when it went missing in transit between the respondent's offices, located in two different Canadian cities [12]. The complaint raised the issue as to whether the insurance company had in place appropriate security safeguards to protect personal information sent between two of its offices. The company had claimed on its Web site, and in off-line policies, that it administered appropriate security for the personal data in its custody.

The OPC investigation revealed a loss of sensitive medical and other personal information under the control of the respondent, whose measures for the control and tracking of sensitive group insurance files at the time of the incident were found not to meet the requirements of Principles 4.7 and 4.7.1 of PIPEDA. As a result of the complainant's experience, the insurance company re-assessed its procedures and implemented a more secure process for the registration and transfer of insurance files, including the scanning of insurance files and their transfer to authorized employees via an encrypted Web site. The complaint was determined to be *well-founded and resolved*.

If the same situation arose in the U.S., the customer would likely receive a notification from the insurance company, as is required in most U.S. states by state data breach laws. Although these state laws vary somewhat [13], in general they require companies to provide notice to individuals when their data has been compromised as a result of a security breach; in many states, and depending upon the scope of the breach, notice must often be given to the Attorney General and to the media.

If the companies do not inform individuals of the breach, they may be liable to civil penalties (*e.g.*, up to US$500 for each customer not notified). State laws may also allow individuals to sue for damages, which may be defined as actual economic damages; however, in other states, the law only provides for enforcement by the Attorney General [14]. The laws also either require or recommend practices that the company should follow for responding to a data breach.

The individual in this case may also receive notice and have some redress under federal law because the breach involved medical information. The *Health Insurance Portability and Accountability Act of 1996* (HIPAA), as amended by the *Health Information Technology for Economic and Clinical Health Act* (HITECH), requires health insurance plans, health care clearinghouses and health care providers to provide notice to the individual and Secretary of Health and

Human Services (HHS) if there is a security breach involving protected health information; notice to the media is required if over 500 records have been compromised [15]. However, these "breach notification" regulations are enforced by the HHS Secretary; HIPAA does not permit a private right of action. Additionally, the U.S. Federal Trade Commission (FTC) has issued companion breach notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA [16].

*Case Four: Hotel discloses a guest's check-in and check-out times to his employer*

The complainant lost his job after a hotel verbally provided his business travel check-in and out times to a private detective working for his employer during an investigation into whether employees were claiming overtime unnecessarily [17]. The Commissioner found that check-in and check-out times were the employee's personal information and had been disclosed neither with his consent nor under circumstances for which PIPEDA would authorize the organization to disclose without his consent. Nowhere on the hotel's Web site was the consumer notified that this was a possible disclosure of personal information.

The OPC determined that the complaint was well-founded, and the hotel reviewed and revised its policy and communicated it to hotel employees. The revised policy clarified the very limited circumstances under which guest information could be released and suggested that disclosure decisions go through management wherever possible.

The investigation found that the following parts of PIPEDA had been contravened: Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate; and paragraphs 7(3)(c.1) and (d) of PIPEDA outline limited circumstances wherein personal information may be disclosed to a government institution or investigative body, for reasons of national security or for the purposes of enforcing or administering a law, which were not met. The OPC concluded that the complaint was *well-founded and resolved*.

Hotels in the U.S. are not required to have privacy notices or to comply with any federal regulations. Some U.S. hotels do post privacy notices but these tend to be the larger chains, especially chains that also operate outside the U.S. In general, hotels collect a fair amount of rather detailed information about guests, including contact and payment information, room preferences, travel and car information and details of other individuals in a guest's party.

Some states and localities have laws or ordinances requiring hotels to collect certain information. For example, Los Angeles "requires hotel and motel operators to collect and record detailed information about their guests in either paper or electronic form. The records must contain: the guest's name and address; the number of people in the guest's party; the make, model, and license plate number of the guest's vehicle if the vehicle will be parked on hotel property; the guest's date and time of arrival and scheduled date of departure; the room number assigned to the guest; the rate charged and the amount collected for the room; and the method of payment" (Friedersdorf, 2014). More than 100 cities and counties have a registry-inspection requirement similar to the one in Los Angeles (Gerstein, 2015).

Additionally, courts have recognized that hotel guests have Fourth Amendment protections against unreasonable searches and seizures and that a search warrant would be required to access a guest's room (Hillman, 2014). Recently the Supreme Court ruled unconstitutional another Los Angeles ordinance, which allowed law enforcement to access hotel records without a warrant, because the ordinance did not give the hotel an opportunity to question the reasonableness of law enforcement request. In this case, Los Angeles had argued that motels and hotels were "closely regulated" businesses and thus subject to warrantless inspections [18]. The Supreme Court did not address the requirement that hotels collect specific information on hotel guests.

Fourth Amendment protections only apply against law enforcement and not against an employer's request for check-in and check-out times. However, if a clerk were to give that information to an employer, it is likely that the individual could try to bring a civil suit against the hotel clerk and possibly against the employer. Whether the individual would win such a suit is not clear. Additionally, if a hotel did have a privacy policy that indicated it would not release information to a third party, such as an employer, without the guest's consent or a court order, then the guest could submit a complaint to the FTC — and might be successful in that venue. In 2012, the FTC filed a lawsuit against Wyndham Hotels, as their online security practices did not match their privacy policy (Braun, 2012).

*Case Five: Telecommunications firm does not respond to access requests and destroys personal information subject to those requests*

A complainant who subscribed to Internet and wireless services requested access to personal information held by her mobile telecommunications company, in the form of notes and transcripts of recorded conversations within a date range, to support her position in an account dispute with that company [19]. The Commissioner found that the company did not meet the statutory time limit for responding, destroyed the requested information in the course of regular information management before the individual's recourse was exhausted, had internally inconsistent policies in place and had not properly trained employees.

Principle 4.9 states that upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. The OPC has issued guidance for recording an individual's personal information in phone calls.

Principle 4.9.4 states in part that an organization shall respond to an individual's access request within a reasonable time and at minimal or no cost to the individual. The complainant's first access request did not elicit a response; she followed up, yet during that time her account was turned over to a collection agency that contacted her to collect a debt. According to an employee, transcribing the call would be too costly; the parties instead settled on, and the complainant paid, a lower final amount. The organization undertook to correct her personal information on file with the collection agency, as obliged by PIPEDA's Accuracy Principle, but the collection action continued for some time and her access request continued to be unanswered.

Principle 4.1.4 states that organizations shall implement policies and practices to give effect to the principles, including ... (c) training staff and communicating to staff information about the organization's policies and practices. The OPC found fault with the company's policies regarding retention of personal information subject to an access request and responding to such requests regardless of efforts to settle an underlying dispute. It also found that the company's policies for responding to personal information requests for phone calls had neither been followed nor properly communicated to employees, despite a similar case against the company previously.

The Commissioner's preliminary report recommended that the company amend two policy and procedure documents and submit them for review by the OPC and also submit a clear and detailed training and communications plan to educate employees. The company took the action. The complaint was reported as *well-founded and resolved*.

Procedures for accessing and correcting an individual's records with a telecommunications provider in the U.S. are not as clearly spelled out for telecom customers as they are in Canada. Many cellular providers, like Verizon, combine cellular packages with Internet, land-line, and cable services; for this reason, the *Cable Communications Policy Act of 1984*, as amended by the *Cable Television Consumer Protection and Competition Act of 1992*, may have some relevance. It contains typical fair information practices for subscriber privacy, including the right to access personally identifiable information at reasonable times and at a convenient place with reasonable opportunity to correct information.

Further, a cable operator is required to destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information. The Act also gives individuals the right to bring civil action in federal court if they believe these rights have been violated. State laws may provide a similar right of access and correction with similar rights to sue [20]. The Act does not specifically require staff training or other mechanisms of accountability.

Additionally, the *Telecommunications Act of 1996* requires telecom companies to ensure that Customer Proprietary Network Information (CPNI) is not disclosed to a third party without consent. CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and ... information contained in the bills ... ." (Privacy Rights Clearinghouse, 2014). The Act does not provide any individual rights of access or correction.

The Federal Communications Commission (FCC) has jurisdiction and enforcement power over the Cable Act and the Telecommunications Act, and may provide another avenue for individual complaint. The FCC has received complaints from customers about unauthorized access to records (especially relating to pretexting) and that companies were not properly training, monitoring and disciplining employees [21]. There have also been lawsuits by state agencies against data brokers who access telephone records through pretexting. The FTC has also received complaints about telecom providers' unauthorized disclosures of information without individual consent. Whether the FCC, the FTC or state agencies would provide an avenue for successful resolution of an individual's complaint regarding access to notes and transcripts about a billing dispute, as well as questions about time limits and staff training, is very unclear.

As with the prior cases, state consumer protection and cable/telecommunications laws may also provide an avenue for redress and state AG offices may provide a forum to which one could submit a complaint.

**Conclusions**

These five cases, from different sectors and reflecting an array of privacy issues, expose some clear contrasts between processes for redress for privacy harms in Canada and the United States.

The first obvious difference is that there is a single point of contact for privacy complaints in Canada. The argument should not be overstated. The Canadian federal system is complex, and other federal agencies in Canada also have responsibilities for privacy protection: the Canadian Radio-Television and Telecommunications Commission (CRTC), for instance, has responsibilities for enforcing telemarketing rules, the Do-Not-Call-List and the new Canada Anti-Spam legislation (CASL). The salient point, however, is that if a complainant went to the OPC with an issue that was not within its jurisdiction, it would typically be able to refer that individual to the relevant provincial or federal agency, and it even has online tools to help the individual [22]. The OPC therefore serves as an important clearinghouse for privacy complaints and as a central authority for the interpretation of the law and the provision of guidance to organizations about compliance.

The situation is obviously far more fragmented and complicated in the U.S. Firstly, it is more difficult in the U.S., for an individual to determine if what they perceive as a privacy violation is actually illegal. These five cases, in themselves, have revealed the potential responsibility of numerous federal and/or state agencies. For some cases, the potential authority is also distinctly hypothetical and contingent. As in Canada, an American consumer could complain free of charge to any number of agencies about a privacy violation, but there would be far less guarantee that the agency would have the authority, expertise or inclination to investigate. Most would have many other statutory responsibilities beyond privacy protection.

The individual might also choose to complain to multiple agencies, but the potential for "getting the run around" would be significant. It is likely that the individual in the U.S. will become frustrated by the number of potential routes and the lack of clarity about probable success — unless he or she is intensely aggrieved and feels passionately about having "justice" done. The burden is on the individual and entails time, energy and, in many cases, money.

Secondly, and relatedly, the comparison of likely case resolution in the U.S. and Canada highlights the critical importance of privacy expertise. A full-time staff of around 180 now supports the Canadian Privacy Commissioner and has developed significant knowledge of the range of legal, technical and social questions that this complex issue raises.

The OPC is, to be sure, always short of technical expertise but is gaining expertise on a range of privacy issues as illustrated by the investigation of the Google ads case, which involved a complex technical audit of Google's remarketing platform. When further expertise is needed, the OPC can hire on contract.

There is, of course, considerable privacy expertise within the U.S. government, especially in federal agencies responsible for U.S. government programs — but this expertise is dispersed in bureaus and branches often deep within larger federal agencies. We note, moreover, that it was only rarely that the fact situations encountered in the cases above really involved one of the more established privacy oversight offices within federal agencies.

It is also notable how often the potential involvement of state AGs was mentioned. Citron's recent work (2016) on the role of state AGs reveals more privacy activity than is commonly assumed, proposing legislation, using persuasion, promoting publicity and pursuing litigation. It also describes cooperation among the states through the Privacy Working Group of the National Association of Attorneys General, as well as multistate privacy efforts against national companies. She concludes, in part, that: "attorneys general serve as crucial partners, dissenters, and enforcement gap fillers *vis-à-vis* federal agencies" [23]. These offices also receive complaints about privacy, and have wide-ranging authority over many other state regulatory questions.

The FTC might potentially also play a role, and has developed significant privacy expertise. However, its authority extends only to cases where "unfair and deceptive" trade practices under Section 5 of the FTC Act can be proven and where there is a pattern of such practices rather than an individual complaint — a high threshold (Hoofnagle, 2016). The FTC has levied some significant fines for corporate privacy breaches over the seven to eight years, and indeed significantly more than has ever been, or probably will ever be, imposed by any Canadian court [24].

Thirdly, the more widespread legislative coverage of the private sector in Canada is clearly an advantage to the average individual. The coverage is still not comprehensive, as there are some organizations (mainly non-profit) that fall between the cracks of a legal regime that either applies to government agencies or to commercial organizations. That said, the vast majority of organizations, and especially those that are the most privacy invasive, are caught under one law or another. With respect to the private sector, this means that the regime does not have to tackle thorny questions about where one sector begins and another ends. The laws are not 100 percent compatible with one another (particularly in the health field), but they are close.

The cases obviously portray a very different picture in the U.S. Of the five cases, none was clearly covered by a federal privacy statute. The case on the insurance privacy breach would probably receive redress in many states. Of the others, it is not obvious whether any (or which) state or federal law definitively provides legal privacy obligations to the company concerned, or rights of redress for the individual.

These cases clearly highlight the problem of 'sectoral' regulation. All these cases are hybrids, especially those involving online activity. Is Case One about marketing, health, or online search? Is Case Three about insurance information or health information? Is Case Five about the telecommunications or cable industries? The U.S. approach to private sector privacy protection has largely been based on an assumption that privacy issues and relationships vary from sector to sector, and therefore require different statutory rules. That theory is under increasing strain as companies offer larger suites of products and services online, as media convergence produces a range of hybrid organizations, and as business-to-individual relationships and roles are not as easily compartmentalized as in the past.

Finally, the U.S. approach places a heavy responsibility on the individual to use his or her initiative to find an appropriate avenue of recourse, and typically that will require expensive and time-consuming litigation. In Canada, at least initially, the individual's voice can be heard and the organization called to account for its practices. However, if the Commissioner finds for the organization, the individual then only has recourse to the courts — again an expensive proposition. Even if a complaint is well-founded yet the organization refuses to change its practices, the Commissioner can also then resort to the courts. However, the OPC has a limited budget for legal services, which sometimes pales in comparison with that of large multinational enterprises. The reality is that, despite the advantages of the ombudsman model, some high-profile battles over the meaning and interpretation of the law are going to be resolved in the Canadian courts with similar barriers to entry as in the U.S.

The analysis of these cases reinforces a central conclusion that privacy protection in the private sector in the U.S. is still heavily dependent on self-regulation through company and industry codes of practice. In each of these scenarios, the behavior of equivalent US companies would likely by governed by a number of organizational or sectoral privacy policies. The online advertising industry, for instance, is covered by the Network Advertising Initiative code of conduct [25]. There are also examples of privacy codes for the insurance, telecommunications and hotel industries, which might allow opportunities for consumer redress. Bamberger and Mulligan (2015) have stressed the importance of self-regulatory initiatives that drive corporate behavior through "privacy on the ground." There has been some extensive activity by U.S. corporations over the last 20 years: thousands of chief privacy officers; a professional association; flourishing legal, auditing and consulting practices; and privacy seal and certification programs.

We suspect, however, that this activity is stimulated less by an increased recognition that privacy is a widespread and fundamental right, and more by the view that the mishandling of personal information is a 'risk' that needs to be 'managed.' In a risk management culture, consumer complaints are regarded less as an essential expression of the right to control one's personal information, and more as something to be minimized. Criticisms of self-regulation in the United States have been long-standing and persistent (Turow, *et al.*, 2014).

Self-regulatory initiatives still play an important role within the Canadian system. The difference of course is that self-regulation in Canada is conducted within the framework of an over-arching statutory framework that produces more consistency across sectors, corrects for market failures, and provides an opportunity for redress to an independent officer of parliament if self-regulation is perceived to fail. Those same arguments seem to be at the heart of the Obama Administration's 2012 initiative for a "Consumer Bill of Rights" (White House, 2012).

We concede that a more comprehensive and systematic study is necessary across a more representative sample of cases to substantiate these claims more fully. We would, however, insist that this analysis of real problems raised by

ordinary individuals is at the heart of the philosophy and politics of privacy protection. Some of the cases may seem mundane, and none resulted in the award of monetary damages. However, they were significant to the Canadians who took the trouble to complain to the OPC. These individuals were exercising their basic rights to control the circulation of their personal information, online and off-line. That claim for information privacy is as powerful in the United States as it is in Canada.

**About the authors**

**Colin J. Bennett** is Professor of Political Science at the University of Victoria, B.C., Canada.
Direct comments to cjb [at] uvic [dot] ca

**Priscilla M. Regan** is Professor of Government and Politics at George Mason University.
E-mail: pregan [at] gmu [dot] edu

**Robin M. Bayley** is President of Linden Consulting, Inc. in Victoria, B.C., Canada.
E-mail: rb [at] lindenconsult [dot] ca

**Acknowledgments**

We acknowledge the very useful research assistance of Kate Newman, Ph.D. student at the University of Victoria. An earlier draft of this paper was presented at the Privacy Law Scholars Conference in 2016. The authors are grateful to Bob Gellman for his thoughtful comments on that occasion.

**Notes**

1. Bamberger and Mulligan, 2015, p. 8.

2. Bennett and Raab, 2006, p. 265.

3. PIPEDA Fair Information Principles at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/, accessed 21 December 2016.

4. OPC's Tips for Raising Privacy Concerns with an Organization at https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/raising-your-privacy-concern-with-an-organization/, accessed 21 December 2016.

5. PIPEDA Report of Findings #2014-001, 14 January 2014, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-001/, accessed December 21 2016.

6. Libert, 2015, p. 6.

7. The NAI Code of Conduct, Network Advertising Initiative, at http://www.networkadvertising.org/code-enforcement/code, accessed 21 December 2016.

8. DAA Self-Regulatory Principles, Digital Advertising Alliance, at http://www.digitaladvertisingalliance.org/principles, accessed 21 December 2016.

9. PIPEDA Report of Findings #2013-015, 18 December 2013, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-015/, accessed 21 December 2016.

10. These states include: New Jersey, Florida, Texas, Connecticut, Michigan, Ohio, Virginia and Illinois. See http://onlinedatingbackgroundchecks.com/resources/state-laws-about-internet-dating-safety/, accessed 21 December 2016.

11. Joint Statement of Key Principles of Online Dating Site Safety, 19 March 2012, https://oag.ca.gov/system/files/attachments/press_releases/n2647_agreement.pdf, accessed 21 December 2016.

12. PIPEDA Report of Findings #2014-003, 3 March 2014, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-003/, accessed 21 December 2016.

13. For a list and links to specific state laws, see http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, accessed 21 December 2016. The states that do not have security breach laws are Alabama, New Mexico and South Dakota.

14. See Steptoe & Johnson LLP for charts with an extensive compilation and comparison of state and federal security breach laws as of 21 January 2016, at http://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf; and see BakerHostetler's analysis of state security breach notification laws, with charts analyzing key issues in those laws, at http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf, accessed 21 December 2016.

15. Breach Notification Rule, U.S. Department of Health & Human Services, at http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, accessed 21 December 2016.

16. FTC Health Breach Notification Rule, at https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule, accessed 21 December 2016.

17. PIPEDA Report of Findings #2013-007, 7 August 2013, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-007/, accessed 21 December 2016.

18. *City of Los Angeles v Patel*, decided 22 June 2015. For more information, see https://www.oyez.org/cases/2014/13-1175, accessed 21 December 2016.

19. PIPEDA Report of Findings #2012-010, 13 May 2013, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2012/pipeda-2012-010/, accessed 21 December 21 2016.

20. Integrated Cable Act: Communications Act of 1934, at http://www.calcable.org/wp-content/uploads/2013/04/CableCommunications.pdf, accessed 21 December 2016.

21. Protecting Your Telephone Calling Records, FCC, at https://www.fcc.gov/consumers/guides/protecting-your-telephone-calling-records, accessed 21 December 2016.

22. Find the right organization to contact about your privacy issue at https://www.priv.gc.ca/en/report-a-concern/leg_info_201405/, accessed 21 December 2016.

23. Citron, 2016, p. 46.

24. Enforcing Privacy Promises, FTC, at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises, accessed 21 December 2016.

25. The NAI Code of Conduct, Network Advertising Initiative, at http://www.networkadvertising.org/code-enforcement/code, accessed 21 December 2016.

**References**

Kenneth A. Bamberger and Deidre Mulligan, 2015. *Privacy on the ground: Driving corporate behavior in the United States and Europe*. Cambridge, Mass.: MIT Press.

Colin J. Bennett, 2015. "GPEN: A growing network, but how much enforcement?" *Privacy Laws and Business International*, volume 138, pp. 19–21.

Colin J. Bennett and Charles D. Raab, 2006. *The governance of privacy: Policy instruments in global perspective*. Second and updated edition. Cambridge, Mass.: MIT Press.

Christopher Berzins, 2010. "Complaining under PIPEDA: An exercise in futility," *Canadian Privacy Law Review*, volume 7, number 9, p. 104.

Robert E. Braun, 2012. "Hotel liability for guest information — What you need to know and how to avoid liability," *Hotel Business* (12 September), and at http://hotellaw.jmbm.com/liability_for_guest_information_.html, accessed at 21 December 2016.

Canadian Standards Association (CSA), 1996. *Model code for the protection of personal information*. Etobicoke, Ontario: CSA International.

Center for Democracy & Technology (CDT), 2009. "Online behavioral advertising: Industry's current self-regulatory framework is necessary but still insufficient on its own to protect privacy" (December), at https://cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf, accessed 21 December 2016.

Danielle Citron, 2016. "Privacy enforcement pioneers: The role of state attorneys general in the development of privacy law," *University of Maryland Legal Studies Research Paper*, number 2016–08, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297, accessed 21 December 2016.

European Commission, Article 29 Working Party, 1998. "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive," working document (24 July), at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf, accessed 21 December 2016.

Henry Farrell and Abraham Newman, 2016. "The transatlantic data war: Europe fights back against the NSA," *Foreign Affairs*, volume 95, number 1, pp. 124–133, and at https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war, accessed 21 December 2016.

Conor Friedersdorf, 2014. "A hotel's right to protect the privacy of its guests," *Atlantic* (30 October), at http://www.theatlantic.com/politics/archive/2014/10/a-hotels-right-to-protect-the-privacy-of-its-guests/382122/, accessed 21 December 2016.

Michael Geist, 2012. "Privacy commissioner should name leaky websites," *Toronto Star* (29 September), at https://www.thestar.com/business/2012/09/29/privacy_commissioner_should_name_leaky_websites_geist.html, accessed 21 December 2016.

Robert Gellman, 1993. "Fragmented, incomplete, and discontinuous: The failure of federal privacy regulatory proposals and institutions," *Software Law Journal*, volume 6, pp. 199–238.

Josh Gerstein, 2015. "Supreme Court boosts privacy rights in hotel case," *Politico* (22 June), at http://www.politico.com/story/2015/06/hotel-guest-list-privacy-supreme-court-ruling-119280, accessed 21 December 2016.

Roger L. Hillman, 2014. "Guest room privacy and the Fourth Amendment" (12 September), at http://www.duffonhospitalitylaw.com/2014/09/guest-room-privacy-and-the-fourth-amendment/, accessed 21

December 2016.

Chris Jay Hoofnagle. 2016. *Federal Trade Commission privacy law and policy*. Cambridge: Cambridge University Press.

France Houle and Lorne Sossin, 2010. "Powers and functions of the ombudsman in the *Personal Information Protection and Electronic Documents Act*: An effectiveness study," Office of the Privacy Commissioner of Canada, and at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2010/pipeda_h_s/,accessed 30 June 2016.

John Kropf, 2007. "Networked and layered: Understanding the U.S. framework for protecting personally identifiable information," *World Data Protection Report*, volume 7, number 6; version at https://www.dhs.gov/sites/default/files/publications/privacy_networked_layered.pdf, accessed 21 December 2016.

Christopher Kuner, 2014. "EU and US data privacy rights: Six degrees of separation," *Concurring Opinions* (9 June), at https://concurringopinions.com/archives/2014/06/eu-and-us-data-privacy-rights-six-degrees-of-separation.html, accessed 21 December 2016.

Timothy Libert, 2015. "Privacy implications of health information seeking on the Web," *Communications of the ACM*, volume 58, number 3, pp. 68–77.
doi: http://doi.org/10.1145/2658983, accessed 9 February 2017.

Stephanie Miles, 2002. "DoubleClick reaches deal with state attorneys general," *Wall Street Journal* (26 August), at http://www.wsj.com/articles/SB1030381164280449795, accessed 30 June 2016.

Office of the Privacy Commissioner of Canada (OPC), 2015a. "The *Digital Privacy Act* and PIPEDA" (November), at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/legislation-related-to-pipeda/02_05_d_63_s4/, accessed 21 December 2016.

Office of the Privacy Commissioner of Canada (OPC), 2015b. "Privacy protection: A *global affair*, Annual report to Parliament 2014 on the *Personal Information Protection and Electronic Documents Act*," at https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201415/2014_pipeda, accessed 21 December 2016.

Office of the Privacy Commissioner of Canada (OPC), 2014. "Fact sheet: Privacy legislation in Canada" (15 May), at https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp, accessed 21 December 2016.

Office of the Privacy Commissioner of Canada (OPC), 2012. "File a formal privacy complaint," at https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/, accessed 21 December 2016.

Stephanie Perrin, Heather Black, David H. Flaherty and T. Murray Rankin, 2001. *The Personal Information Protection and Electronic Documents Act: An annotated guide*. Toronto: Irwin Law.

Phoenix Strategic Perspectives, Inc., 2016. "2015 Public opinion research with Canadian businesses on privacy-related issues," Office of the Privacy Commissioner of Canada (March), at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016-1/por_fg_201603/, accessed 21 December 2016.

Privacy Rights Clearinghouse, 2012. "Looking for love online: Be aware of the risks" (27 August), at https://www.privacyrights.org/blog/looking-love-online-be-aware-risks, accessed 22 December 2016.

Priscilla M. Regan, 2003. "Safe harbors or free frontiers? Privacy and transborder data flows," *Journal of Social Issues*, volume 59, number 2, pp. 263–282.
doi: http://doi.org/10.1111/1540-4560.00064, accessed 9 February 2017.

Priscilla M. Regan, 1993. "The globalization of privacy: Implications of recent changes in Europe," *American Journal of Economics and Sociology*, volume 52, number 3, pp. 257–274.
doi: http://doi.org/10.1111/j.1536-7150.1993.tb02546.x, accessed 9 February 2017.

Joel Reidenberg, 2013. "Should the U.S. adopt European-style data-privacy protection?" *Wall Street Journal* (10 March), at http://online.wsj.com/news/articles/SB10001424127887324338604578328393797127094, accessed 21 December 2016.

Rainey Reitman, 2012. "Six heartbreaking truths about online dating," *Electronic Frontier Foundation* (10 February), at https://www.eff.org/deeplinks/2012/02/six-heartbreaking-truths-about-online-dating-privacy, accessed 21 December 2016.

Cristin Schmitz, 2016. "Privacy watchdog wants to see new office enforcement muscle," *Lawyers Weekly*, volume 26, number 4 (27 May), and at http://www.lawyersweekly.ca/articles/2683, accessed 21 December 2016.

Sidley Austin LLP, 2016. "Essentially equivalent: A comparison of the legal orders for privacy and data protection in the European Union and the United States" (25 January), at http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf, accessed 21 December 2016.

Joseph Turow, Amy Bleakley, John Bracken, Michael X. Delli Carpini, Nora A. Draper, Lauren Feldman, Nathaniel Good, Jens Grossklags, Michael Hennessy, Chris Jay Hoofnagle, Rowan Howard-Williams, Jennifer King, Su Li, Kimberly Meltzer, Deirdre K. Mulligan and Lilach Nir, 2014. "Americans, marketers, and the Internet: 1999–2012," *Annenberg School for Communication, University of Pennsylvania, Working Paper* (1 May), at at http://repository.upenn.edu/asc_papers/348, accessed 21 December 2016.

U.S. Department of Health, Education & Welfare (DHEW), 1973. "Records, computers and the rights of citizens," *DHEW Publication*, number (OS)73–94. Washington, D.C.: U.S. Department of Health, Education & Welfare; version at https://www.justice.gov/opcl/docs/rec-com-rights.pdf, accessed 9 February 2017.

U.S. Federal Trade Commission (FTC), 2010. "Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers," at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf, accessed 21 December 2016.

U.S. Mission to the European Union, 2013. "Data privacy: Five myths about the US legal system," at http://useu.usmission.gov/, accessed 21 December 2016.

U.S. White House Office, 2012. "Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy" (23 February), at https://permanent.access.gpo.gov/gpo24557/privacy-final.pdf, accessed 21 December 2016.

Alan Westin, 1967. *Privacy and freedom*. New York: Atheneum.

---

**Editorial history**

Received 7 June 2016; revised 23 December 2016; accepted 9 February 2017.

---



If these Canadians lived in the United States, how would they protect their privacy?
by Colin J. Bennett, Priscilla M. Regan, and Robin M. Bayley.
*First Monday*, Volume 22, Number 3 - 6 March 2017
https://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/6817/5919
doi: http://dx.doi.org/10.5210/fm.v22i13.6817