

Privacy International Response to British Columbia Information & Privacy Commissioner

August 2004^[1]



Summary of Points

The Privacy Commissioner for British Columbia made a call for submissions on whether the USA PATRIOT Act could allow the U.S. authorities to gain access to Canadians' personal information, enabled through the outsourcing of Canadian public services to the United States. The Commission also called for comments on the implications for compliance with Canadian provincial privacy laws, and to see if anything could be done to eliminate or mitigate the risks.

In this submission to the BC Commissioner, we contend that the USA-PATRIOT Act does allow access by U.S. authorities, as do many other laws within the U.S. and other agreements between the U.S. and Canada. Moreover, Canadian laws and practices are as equally invasive as the USA-PATRIOT Act, and also provide access to this personal information by other foreign entities.

In response to this state of affairs, we call for a renewed discussion and debate to re-invigorate privacy protections lest they become ineffective in this *new* environment. Canadian laws were created to protect privacy and civil liberties, and yet they are often in vain. Fighting terrorism is legitimate; applying terror rules to non-terror-related situations is dishonest, and we ask that this situation be fixed. Failing that, the trust and faith of Canadian citizens in their laws and in their human rights protections will continue to erode, even as these Canadian laws and practices are copied by other countries. This practice is corrosive to human rights internationally.

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, police information systems, medical privacy, and freedom of information and expression. Prominent members of our advisory board are Canadian, and have played roles cultivating and nurturing the strong culture of privacy in Canada, and on the legislative

landscape too. Last year we met with the Canadian Parliament Citizenship & Immigration Committee regarding the National ID card system, and participated in the consultation process. Our interest in Canada is thus genuine and long-standing. For more on this, please see <http://www.privacyinternational.org/canada>.

An Open Opportunity

We are grateful that the BC Commissioner's office has opened this area for investigation. It is a timely investigation of a pressing cause. So begins the process of opening the windows to let the sunlight in on the international agreements and national practices that affect Canadians' privacy interests. We can only hope for more of this sunlight, as we are increasingly in need of disinfectant.

Privacy protection has gone through a number of transformations. Previously, we worried about adequate privacy protections in national laws to assure citizens of their privacy in their interactions with public and private entities. Then we focussed on how these protections may exist within the context of trans-border commerce and other activities. These issues are not recent. Laws and international treaties were developed with these concerns in mind throughout the 1960s, 70s, and the early 80s. To make privacy laws effective, an international reach is required.

Now much of our focus is on overbearing laws that invade privacy. These are everywhere, even in countries where there are data protection laws. And so we are finally attending to the national laws that invade privacy with little oversight, scrutiny, specificity, and reporting.

The issue here is that these laws have international effects, and when combined with legacy practices and measures, they reduce privacy protections in Canadian law. Laws passed abroad will affect Canadian subsidiaries, Canadian firms with offices abroad, and Canadian data. This is globalisation in all ways, for better and for worse. As the Geist and Homsy submission states clearly, the powers and practices that allow for such extra-jurisdictional access to personal data arose mostly in the 1970s and 1980s. It is not a development of the 1990s globalisation growth, nor the 2000s dearth in surveillance. Nowadays, to make surveillance effective, an international reach is optimal.

Canadian law is now at the mercy of foreign executive decisions, legislative deliberations, and judicial decisions. We should avoid seeing Canada as a lonely lamb about to be engulfed by the American wolf. The laws that protect privacy in Canada are many and they act as models to the rest of the world. Canada's laws on surveillance, however, are also models of invasiveness. As a number of submissions stated, most remarkably the one from ITAC, Canadian law

enforcement and national security agencies already has similar practices to the Americans. How can Canada turn down another for something that they would choose to allow for themselves? The problem thus begins at home.

Even more worryingly, the Canadian laws that curtail privacy and civil liberties are used by other countries as models. On a number of occasions we observed the use of Canadian statutory language in other countries, word for word. Canada is again a model, although not gloriously so.

Canada, with the leadership of British Columbia, can re-establish itself as a model for the protection of civil liberties. Failing to do so, however, will mean that it will continue to, intentions aside, act as a promoter of greater surveillance and weakened oversight world-wide. And in the meantime, the personal information of those who should be protected by existing Canadian law will continue to be accessible to foreign jurisdictions. And the problem neither begins nor ends with the U.S., as many other countries may also gain access to Canadians' personal information.

What is going on here is that there are greater and greater concerns regarding the increased arbitrariness of the powers of the state. We see new laws, new procedures, and increased closedness, increased international arbitrage, increased use of new technologies to surveil our activities. Yet we also see a decreasing number of adequate protections, with decreasing effectiveness.

The Effects of U.S. Policy

We defer to those who are experts on U.S. law and policy-making to better express the points on how the USA-PATRIOT Act permits access to data stores holding the personal information of Canadians, and Canadian data stores. Others have effectively pointed to other statutes and practices in the U.S. that will also provide U.S. authorities access to these same data stores. What is remarkable is that we are all noticing only now.

Reasonable people may say that the USA-PATRIOT Act is not problematic because of the letter of the law, or it is no different to existing practices and laws. These people are probably right in much of what they say. But within our current legislative and political environment we can not separate the concerns of those who fear anti-terrorism laws but do not know its contents, from the concerns of those who worry about being sent to jails in third-countries because of opaque regimes of international co-operation, from the concerns about not being able to get onto airplanes or open banks accounts because of inaccurate information, or from the concerns of being wiretapped by all-listening ears. Perhaps these fears are not well grounded, but the lack of confidence and the fears themselves are real. Reasonable people may

debate about truth and facts, but the results of such a debate are almost secondary to our decreased confidence that our rights are adequately protected.

The situation may not be legally wrong, but it remains dishonest and sufficiently opaque to all. Much needs to be done to increase our confidence, all these years after so much has been done in the name of increasing our security.

We call for action by the Legislatures to fix this increasingly worrying problem of trust in the protection of personal information. It only makes matters more urgent because the personal information in question is medical information. The collection of this information is already hinged upon the highest level of confidence in its protection. Our call for a legislative fix is a reserved call, however, with some advice for restraint.

Public and Private Data Sharing: Safe Harbours from Scrutiny

For many years, Privacy International has worked to draw attention to the problems in trans-border flows of personal information. In the 1990s we drew attention to the lack of adequate protections in U.S. law, hoping that the European Commission would stand up for privacy protection. The *Safe Harbour* agreement was the result, to our dismay.

We had hoped that the Safe Harbour agreement was a start of a dialogue towards better protections internationally. We have been disappointed repeatedly since then. The disappointment is not only towards the Americans, however. And this is the careful point we wish to make.

Consider the transfer of personal information from non-U.S. air carriers and reservation systems to the U.S. Department of Homeland Security (DHS). When negotiations began in 2002 and 2003 regarding the transfer of this personal information from EU carriers to the DHS, the DHS demands were wild: information would be downloaded by DHS agents and stored indefinitely, or for up to 50 years. There would be no oversight in this process, and few protections on the use of that data.

The European Commission managed to negotiate with the U.S. to prevent the transfer of sensitive data, to minimize its use, to prevent direct access by U.S. officials to the databases and information systems, and minimize the retention period to three and a half years. This can be seen as a remarkable settlement. Perhaps, then, Canada could negotiate a similar agreement on all data.

We are weary of advising this however, on two grounds. First, the 'agreement' established between the U.S. and the European Union is not legally enforceable within the U.S. Any

promises made, any deals struck, are merely words on paper and not legally enforceable. If such an agreement was to be struck with Canada, it would have to be a mutual-legal assistance treaty with legal standing. This is a non-trivial process in U.S. law, as treaties often languish in the U.S. Senate, particularly those treaties that involve minimizing the powers of U.S. law enforcement and national security authorities.

Second, and most importantly, the idea of accessing such personal information was a seed that was planted by the U.S. into the minds of politicians and bureaucrats abroad. The European Commission may have started out with the intent to prevent the transfers of sensitive data and to uphold EU law, but over time its interests transformed. Now the EU is planning to force its own carriers to provide access to this data for EU immigration and border control purposes, and is calling for reciprocity from U.S. carriers. These measures go well beyond the capacities of the U.S. demands and expectations. The U.S. gave the idea to the EU; calling into question EU privacy protections. Once the EU laws were open for negotiation, the EU went ahead and sold away more than it needed in order to advance its own policing powers.

As such we would be hesitant to see such a process begin in Canada where attempts to negotiate with the U.S. regarding means to minimize intrusiveness would instead lead Canada to renegotiate the exemptions in existing privacy laws, and to extend the already expansive powers of law enforcement and national security authorities. Already Canada's amendments to the Aeronautics Act allowed for these transfers to the U.S. with little deliberation in Canada; and Canada has already provided for national access to this data, through Bill C-7 and the Public Safety Act in Spring 2004. When you open the black box of laws and regulations, any number of additional carve-outs may appear. If such a process was to occur in Canada, we would call for clearly articulated expectations and non-negotiable safeguards to be established early on.

Revisiting and Reinvigorating Deliberation

Having started this process of reviewing the extra-territorial powers of the U.S., we believe that the BC Commissioner's office is in the ideal position to establish the conditions for opening up such a forum for deliberation. The time is right to start revisiting the exigencies of previous years, the exemptions established in previous eras. And we must do so with care.

We need to re-evaluate the use of administrative subpoenas in U.S. and Canadian laws and legal practice. We need to examine all existing dataflows between public and private entities, without regard to jurisdiction and nationality, to see if there are clear and just authorization and reporting procedures, if the purposes are clearly explained, if access is specific and constitutional, based on investigations that involve due process, if data integrity and openness is maintained, if there is adequate legal protection for the individuals including consent, and if

balancing criteria represent current legal and technological know-how.

This is indeed the beginning of a complex process. But if we have clearly articulated intentions and safeguards that we are unwilling to negotiate away, then perhaps something can be done. And perhaps much more may be achieved, particularly as this is an opportunity to increase our confidences, and our faiths in protections of privacy and civil liberties that were created in other eras to uphold our faith in our institutions.

Indeed the environment is different from the 1960s when many of these laws and practices were first established in order to protect privacy. The concerns back then included the proliferation of data stores that could amass significant amounts of information; and the threats included the lack of data integrity but also national security concerns amidst the Cold War. Things are significantly different today, with a different technological environment, a different market environment, and renewed and re-invigorated concerns regarding national security and law enforcement.

Terrorism is indeed a threat and laws may be created to deal with these threats. It is not our purpose here to belabour this point, as Canada has passed many laws since 2001 to deal with this new environment. Our point, to relate it back to the discussion above, is that the U.S. may have been acting in the name of terrorism when it demanded passenger information from EU carriers; but the EU responded in calling for measures similar to those in U.S. law, but for the purpose of general law enforcement. Canada acted similarly. This is unacceptable, and this is also quite common: laws passed to deal with terrorism are also used for other purposes. Canada must review its laws and the laws of other countries to ensure that this practice stops.

And so, when ITAC points out that Canadian law is just as invasive as the USA-PATRIOT Act, and that the lowering of legal standards is common, they are right and we must not accept that this is a reasonable situation. When Whitaker notes in his response that U.S. privacy law does not protect non-U.S. persons, and that anti-terrorism powers are being used for non-terrorism investigations, he is right, and this is not a reasonable situation. When the BCCLA argues that MLATs are more likely to be used rather than the USA-PATRIOT Act for access to Canadians' data, they are right but we must not accept that these opaque international regimes are reasonable. When BCFIPA claims that we have no assurances or certainties regarding the use of American powers that have minimal reporting measures, they are right and this must be rectified. When the ACLU points to many other U.S. laws with expansive and sometimes unchecked powers, and when the ACLU then calls for an agreed information sharing regime, they are right but we must be weary that in the process of negotiating such an agreement, Canada may change its demands and reduce its own safeguards even further. This is not uncommon even for Canada, as we have seen with the treatment of passenger information.

Our worry is that with inaction we are heading to the lowest standards for privacy protection. We are calling for action on this, but our second worry is that once re-opened for negotiations, future agreements and legislative fixes will not result in greater protections but only greater carve-outs and exemptions. A clear discourse and deliberation procedure must be established to uphold the constitutional rights of Canadians in the face of all these interests and principles, and resulting conflicts.

Concluding Remarks

The legal situation in the U.S. regarding the treatment of personal information is indeed appalling. It does create a problematic situation for Canadian law, as it did with EU practices. This situation must be fixed. Yet, Canada must also fix its own house. The legal protection of privacy and due process in Canadian law is increasingly problematic, to the point that Canada is in less and less a position to criticize others, even as Canada's laws are increasingly being used as standards for other countries. These conditions are establishing unacceptable risks particularly with an increasingly docile set of legislatures.

The British Columbia Commission, as well as all other privacy and information commissions need to protect the hard fought data protection and privacy laws in light of these developments, in order to protect the regime in Canada from the corrosive effects of international policy dynamics and degradation by internal legislative dynamics. At some point this madness must stop. Someone has to stand up and say that this can not continue. We hope this will begin in British Columbia.

More adequate solutions are required to deal with transborder data flows and we welcome opportunities to work with you in the future to come up with new solutions to this very old problem.

Privacy International, August 2004

1. This submission was written by Gus Hosein, a Senior Fellow with Privacy International. At PI he directs the *Terrorism and the Open Society* research programme, and in co-operation with the American Civil Liberties Union, he is running the *Policy Laundering* project. He is a Fellow in the Department of Information Systems at the London School of Economics and Political Science, where he also received his PhD. Gus also holds a B.Math from the University of Waterloo.