

**TRANSBORDER DATA FLOWS & PRIVACY—AN UPDATE ON WORK  
IN PROGRESS**

7<sup>th</sup> Annual Privacy & Security Conference  
Victoria BC

February 10, 2006

David Loukidelis  
Information and Privacy Commissioner for British Columbia

Good morning everyone. With thanks for the kind introduction, I'd like to add my own welcome to our visitors to Victoria, to British Columbia and to Canada.

My welcome, including as it does Canada, recognizes that many of you are visiting from outside the country. There are a good number of you from the United States, while others come from further abroad, including the United Kingdom, Australia and Germany. I'm grateful to the conference organizers, and I suggest we should all be thankful to them, for again broadening the conference's scope. Each year, this event grows in size and each year it grows more and more international in scope.

I welcome and encourage this because it's part of the free flow of ideas and knowledge from around the world about privacy and the various contexts in which it exists. This sharing of ideas, this flow of

information, of course, both imitates and reinforces the increasingly international aspects of privacy protection in an ever-more-connected world.

My goal today is, to be candid, a modest one. My aim is simply to share with you some observations, not original insights, about issues associated with privacy and transborder flows of personal information. My objective is to simply give you a brief overview of a long-developing and very complex set of challenges.

Privacy protection in the context of transborder data flows is, of course, only one of many challenges associated with globalisation. Just as the question of what, if any, environmental protection standards should be fashioned and promoted internationally, discussions around what privacy, or data protection, standards should apply internationally continue some 30 years after they began.

Transborder flows of personal data are nothing new, of course. Personal information flows across borders have been part of international commerce and individual life for centuries. Today, each of us must expect, must know, that every time we order goods from a merchant outside the country, some of our personal information crosses the border—or crosses borders. More and more, however, our personal

information crosses borders when we're doing business only in our own country—or think we are.

For example, if I send an email across town, it's likely to reach its recipient having first travelled outside the country, perhaps even around the world.

To take another example, if I use my credit card to buy something from a bricks-and-mortar merchant in Canada, the card issuer will likely ship my personal information abroad for processing.

A third example of international data flows, has to do with a flight back to Victoria that David Flaherty and I recently shared. When we arrived at the airport, I offered to help David, who's my senior, and grabbed a suitcase off the belt that *I thought* he'd said was his. It weighed a ton and almost broke my back hauling it to the cab. Long story short, it wasn't Flaherty's bag—when David got out of the cab at his house, he said “That's not mine. I thought it was yours”. And I said, “No, you said it was yours.” After we bickered for a while, I called Air Canada's baggage services and gave up our personal information to a very nice gentleman in Mumbai, where at least some of Air Canada's baggage tracking services are handled. No fault of his own, he was no help to us, but he did collect my data and David's, too.

(By the way, I did manage to find the bag's owner and delivered it to him that night. He said he'd seen me walking away with his bag at the airport, but hesitated to say anything. Go figure—it was a late night flight from Toronto, but I don't think Flaherty and I were looking that rough. And then I asked the guy what was in the bag. He said it was full of Bibles, which allowed me to tell David later that that was the closest he's ever going to come to salvation.)

*Anyway*, I digress somewhat, although this example and the other examples I've just given you all illustrate in small but I believe meaningful ways the remarkable ongoing globalisation of information systems and activities. This globalisation of information is associated with advances in information technologies and changes in the nature of the global economy. At the same time, the globalisation of information flows is an ever-more vital driver of economic development and international economic interdependence.

In turn, the interests of economic development and the fact of increasing economic interdependence continue to drive the search for harmonized global privacy standards and compliance oversight mechanisms. The central question in that endeavour is, "What privacy standards should

apply to the transfer of personal data, and to its use and protection, wherever the data might end up?”

Each of us here today has a direct stake in ensuring that transborder data flows can continue as efficiently as possible, but with there being appropriate levels of privacy protection following the flows. The question of what privacy standards should apply to the transfer of personal data, and how, is far from new question, and I’d like to spend a few minutes now describing in broad strokes some of the approaches that have been tried over the years—decades, in fact—in addressing transborder data flows and privacy.

More than a quarter of a century ago, the OECD—the Organization for Economic Cooperation and Development—adopted what remains a leading set of principles for protecting privacy. The OECD’s work built on work of the Council of Europe in the 1970s, which sought to promote harmonization in the privacy, or data protection, laws that were being adopted across Europe. Building on the Council of Europe’s work, the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* remain an important international standard in privacy protection.

I don't propose to review the Guidelines today. For today's purposes, it is important to underscore the rationale for the Guidelines. They were expressly designed to promote international harmonization of privacy protection while protecting the free flow of personal information. They expressly acknowledged the growth of transborder data flows and their implications for both privacy and commerce. They explicitly recognized the need to forestall inappropriate barriers to transborder data flows and thus economic activity. These features of the Guidelines are illustrated by the following quote from the preface to the Guidelines:

...there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data.

Five years after the Guidelines were issued, the OECD issued a declaration that again acknowledged the growth and importance of

transborder data flows. “Flows of computerised data and information”, the declaration said, “are an important consequence of technological advances and are playing an increasing role in national economies. With the growing economic interdependence of Member countries, these flows acquire an international dimension”, the declaration added. The recognition of increasing economic inter-dependence—and remember, this was 20 years ago—prompted the OECD’s members to commit in 1985 to work on four main objectives:

First, to promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;

Second, to seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows;

Third, to develop common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonized solutions;

Fourth, to consider possible implications for other countries when dealing with issues related to transborder data flows.

So, where are we, more than a generation after the OECD’s Guidelines and its solemn declaration of commitment to solve the challenges of transborder data flows? And, once we understand more or less where

we are now with global privacy protection, the next question is where are we headed?

After the OECD Guidelines came out, European countries carried on adopting their own data protection laws, undoubtedly influenced to some degree by the Guidelines. While Europe's data protection laws bear some similarities to Canada's second generation laws, many of the Continental versions share a feature not found here in Canada, namely, the licensing of organizations that handle personal information and the control of exports of data.

Austrian law, for example, requires one to obtain a licence to transfer personal information abroad, with the licence being recorded in a public registry. A licence will be refused where the country to which the information is to be sent does not offer sufficient protection for personal information. A similar approach applies in France, whose data protection authority can refuse permission to export data to a country where there is no privacy protection the authority considers equivalent to that offered in France. Sweden and Finland take comparable approaches to data transfers.

More recently, the EU as a whole moved to harmonize and export an approach to privacy through its 1995 Directive on personal data

protection. Under the Directive, which required all EU member states to bring their national privacy laws into line with the Directive's standards, the export of personal data may be prohibited where the receiving country hasn't got an equivalent level of data protection.

Prohibitions on the export of personal information proceed from a recognition of the challenges that globalization presents to national jurisdiction over behaviour. Generally speaking, a country cannot exercise its legal authority outside its borders, yet so much of the country's economic life and vitality depends on the flow of information back and forth. Regulation of data export therefore recognizes the territorial limits of each nation, but it can also threaten the efficient flows of data across borders.

Not surprisingly, the business community has long had reservations about aspects of the European approach, fearing exactly the kinds of unnecessary barriers to the flow of personal information the OECD Guidelines aim to avoid. The US, as well, has had concerns about the Directive's approach. In 2000, the US and the EU agreed on the so-called Safe Harbor accord, under which US companies can commit to respecting the Safe Harbor version of the EU Directive's principles, with the US FTC enforcing compliance with Safe Harbor.

There are encouraging signs, as well, that the EU and the global business community are, tentatively at least, learning to work together to some degree. For example, they have worked together on model contracts governing the export of personal information, to permit export while using the contract clauses as the privacy framework that, in effect, follows the personal information. Early last year, the Working Party of EU data protection authorities established under Article 29 of the EU Directive approved of model data export contract clauses prepared by the ICC.

This approach to data protection to some extent represents a shift away from traditional models of centralized, state-driven enforcement. Under the contract clauses approach, businesses involved in a data transfer will look to the contract clauses for the rules that regulate their behaviour. They will also look to the contract for dispute resolution mechanisms. As Ralf Bendorath, of the University of Bremen, and others have pointed out, dispute resolution of this kind is more and more the province of massive global law firms brought in by the parties to arbitrate a dispute. This does not by any means entirely displace data protection authorities' role. In fact, it will often be a data protection authority investigation that triggers the dispute between the parties to the transfer, who will look to the contract to sort out responsibility as between themselves.

Similar observations can be made about what are known as binding corporate rules, or global privacy codes. Under this approach, internationally active companies like Microsoft, Oracle or Procter and Gamble will develop a global privacy code for the corporation and then commit to implementing it at the global level. The key is to have the code acknowledged, or even certified, by data protection authorities as meeting local requirements. Observers argue about whether this development—which has received support from the Article 29 Working Party—will lead to a race to the top or to the bottom.

In other words, will global privacy codes adhere to the lowest standards to be found globally, or the highest? As things stand now, at least, I would argue that the race will be to the top. As long as the EU stands firm on the Directive and does not water down its standards, the European market remains important enough that global privacy codes will have to reach up to the EU's requirements.

Will this change? The processes of globalisation are at best murkily understood, and who knows where they will lead? It's now trite to observe that China and South East Asia are rapidly expanding economically. Consumer demand and markets are growing quickly in Asia. Then there's India and its burgeoning population and markets. Will the demographic and economic shift some day soon be such that

European perceptions of privacy, European legal standards of privacy, are not the benchmark for global companies?

Certainly, the APEC economies—including Canada—recognize the need to protect privacy in the context of international commerce and otherwise. In November of 2004, APEC leaders endorsed the APEC Privacy Framework, which sets out key privacy principles in a manner similar to the OECD Guidelines of 25 years ago. The APEC framework commits member economies to adopting national legislation, or other privacy protections, that are consistent with the framework principles.

Now, the framework has been criticized in some quarters as being too light—it's been called "OECD light" by some. It has also been criticized—by Graham Greenleaf of Australia, for example—as having been developed furtively, with insufficient input from NGOs and others.

I acknowledge the valid criticism that many international initiatives to develop technical standards or policies are not sufficiently transparent or inclusive. The ICAO's development of biometric passport standards and state-to-state negotiation of the Cyber Crime Treaty offer two examples of this problem.

Let me pause here and note, as an aside, another important development in global privacy issues. In recent years, particularly, NGOs, both business and not-for-profit, have started to play more of a role in the formulation of standards or rules. Groups such the Global Business Dialogue on E-commerce—a largely Japanese initiative—and the Center for Information Policy Leadership in the US are only two examples of NGOs funded by business members that participate in various ways in global privacy issues. In the not-for-profit community, as well, you have organizations like the European Digital Rights Initiative, and the Electronic Privacy Information Center and the ACLU in the US. To the extent that non-governmental organizations such as the OECD and APEC are active in creating standards or policies around data protection, the involvement of civil society and business groups introduces an important element of inclusiveness, transparency and accountability, all of which enhance quality and legitimacy.

Returning to the APEC framework and criticisms that it is OECD light, whether or not NGOs were invited to sit in the room, I will note that a consultation draft of the APEC framework was made public and submissions were sought.

As for the substantive merits of the APEC framework, my own view of it—and I should disclose here that I was involved in a small way in the

framework's development—is that the framework succeeds in committing Asian economies to privacy protection. Something that would not, in my view, otherwise have happened.

Now, it may be that the global business community will take the APEC framework to the EU and, noting that the EU compromised on Safe Harbor, suggest revisions to the Directive to harmonize it with the more recent APEC work. Signs are, however, that it is more likely the OECD that will step up to the plate. My federal colleague, Jennifer Stoddart, has been active in OECD issues and I know that she is involved in work that would attempt to harmonize the OECD Guidelines with APEC's more recent work. We are at the early stages of this, but I'll watch progress on this front with interest.

Returning to a theme I touched on earlier, a key element of any OECD work in this area is transparency and inclusiveness. Privacy remains, as others have observed, very much an expert's domain. Data protection authorities and supra-national organizations must find ways to ensure legitimacy for their work, and enhance its quality, by embracing, not shunning, the opportunities to engage NGOs and citizens, to create, as Ralf Bendrath put it, new kinds of public spheres around privacy dialogue and to seek input as rules and standards are negotiated.

I've been talking a lot about development of international privacy protection standards, whether public sector or private sector driven. What about enforcement? It's well and good to say that forms of regulation are emerging that can cross borders with the data to which they relate. It's also encouraging that, through binding corporate rules and model contract clauses, the private sector is more and more enabled to self-police. But as I indicated earlier, data protection authorities will not be entirely displaced, and nor should they—and I say this not by way of protectionism for me and my commissioner friends.

Yet, as I've said already, the territorial limits on jurisdiction are very real and threaten the ability of data protection authorities to do their work in the context of international data flows. I am therefore encouraged by one aspect of the APEC framework that is moving ahead this year and perhaps next. Part II of the APEC framework commits member economies to find ways to encourage and facilitate communication and co-operation in enforcement of privacy protections across the region.

A small working group of economies, including Canada, has been formed to model possible solutions to this challenge of globalisation. The group's work is focussed on inter-jurisdictional co-operation among data protection authorities in investigating and enforcing compliance

with privacy requirements. This focus recognizes that harmonization of standards is not the end of the exercise—data protection authorities can and must play a critical role in protecting privacy, but in a way that as far as possible standardizes approaches to privacy. Canadian data protection authorities have for the last few years been working together in a similar fashion and I hope that our work here can support APEC’s efforts in this area.

So, I’ve outlined where we’ve come from and where I believe we are, globally, in data protection. Where are we heading? The Montreux Declaration last year by international privacy and data protection commissioners called for development of global privacy governance instruments and business leaders will continue to seek this as well. In this context, I believe that, over the next five to ten years, we’ll see significant changes in the international governance of privacy. The hybrid forms of privacy governance, as some political scientists have called them, will continue to evolve and probably diversify (particularly if the World Trade Organization becomes involved). We’ll see a combination of private sector instruments coming more to the fore, without the public sector, top-down model of enforcement being displaced. The challenges of transborder data flows will not go away—they’ll probably grow greater—but I do think we have some cause for optimism that innovative privacy governance approaches will be found.

Still looking ahead, the real challenge, in my view, is less transborder data flows in the private sector than the seemingly inexorable appetite for governments everywhere to, in the name of public safety, to gather more and more personal information, amass it in databases and to share it across borders with other national security and law enforcement agencies.

Here in Canada, evidence before the public inquiry into the Maher Arar affair suggests that Arar's personal information was shared with US authorities contrary to the terms of a Canada-US information-sharing agreement, perhaps leading to Arar's captivity in Syria. This illustrates the fact that, no matter what agreements or frameworks are in place, accidents and abuses will happen. But, particularly as regards government-to-government information-sharing, we must insist on appropriate protections for our personal privacy and other liberties and rights.

Thank you for your attention. I'd be happy to take your questions.

\* \* \*