What Happens when you buy an Airline Ticket? Surveillance, Globalization and the Regulation of International Communications Networks

Colin J. Bennett
Associate Professor
Department of Political Science
University of Victoria
Victoria, B.C. V8W 3P5

CJB@Uvic.ca
http://web.uvic.ca/poli/bennett/

Paper prepared for presentation to the 1999 Annual conference of the Canadian Political Science Association, Sherbrooke, PQ, June 6, 1999

Introduction

The ill-defined and controversial phenomenon of "globalization" is now central to the contemporary literature on comparative public policy and international political economy.[1] Embodied within this multi-faceted concept have been a variety of interconnected themes: that globalization represents the latest unfolding of the tension between capital and its social and political foundations; that it shifts power from national authorities to international power structures; that it signifies a triumph of private over public interests; and that it represents a victory for neo-liberal ideas and forms of production (Gill, 1995). Regardless of larger disputes concerning the sources, meaning and effects of this phenomenon, there is perhaps a quite orthodox hypothesis at the root of this entire theory: the sheer volume of cross-border flows of products, people, capital and money has produced a global economy and a concomitant demise of the state's autonomy and of national economic power (Ohmae, 1990). Thus Susan Strange has pronounced the "retreat of the state" as a result of the "impersonal forces of world markets, integrated over the postwar period more by private enterprise in finance, industry and trade than by the cooperative decisions of governments" (Strange, 1996, p. 4).

There are, on the other hand, the sceptics. Some argue that globalization is mere rhetoric. Others claim that is merely neo-liberal ideology. Some concede that the world is changing, but dispute that fact that this change amounts to globalization. Others regard the entire hypothesis as over-generalized and have stressed the continued importance of national regulation as an empirical finding, and a desirable normative condition (e.g. Hirst, 1997; Weiss, 1997). Some comparativists stress that globalization is a multi-faceted and multidimensional phenomenon, and have sought more contingent theoretical generalizations about the effects of globalization on regulatory policies (e.g. Vogel, 1995). Others have critiqued the arguments of both the "hyper-globalization" school and of the sceptics as being based on a view that globalization is an end-state, rather than a continually shifting process (Perraton et al. 1997).

Another orthodoxy, prevalent in somewhat different areas of social science, is that we live in an "information society." This concept too has a variety of mythic and ideological representations. In its popular manifestation, the concept is simply used as a short-hand to describe some the fundamental effects of new information and communications technologies (Negroponte, 1995; Toffler, 1981). Whether indeed the information society represents a structural transformation in late capitalism is also the subject of a more profound debate in the scholarly literature (e.g. Beniger, 1986; Castells, 1996). I do not need to enter this debate in this paper to emphasize the simple point that information clearly flows more freely, knows fewer national attachments, and indeed represents one of the significant forces behind the equally ill-defined processes of globalization.

[1] I am very grateful to David Todd for helpful research assistance, and to my colleague Michael Webb for valuable suggestions about the globalization thesis.

However, hypotheses about globalization tend to be based, not on research into the control over information, but on studies of the flow of money – foreign direct investment, capital mobility, trade balances and so on (e.g. Cerny, 1994). This is unsurprising since, in political science at least, the thesis has primarily been debated amongst students of comparative and international political economy, and is centered squarely within wider disputes between neo-liberal and structural Marxist accounts of international capitalism. Of course, the power of information technology is universally recognized as a crucial force behind the liberalization of financial markets, with concomitant implications for national regulatory and economic power (e.g. Wallman, 1998). But how does the globalization hypothesis fare, when the resource being studied is not money, but information, a commodity that is even more fluid and perhaps difficult for the state to control? The aim of this paper is to submit the basic globalization thesis to examination with reference to a class of policies that concern the flow of information -- not information as "ideas" but information a s a commodity or resource.

For the last thirty years, states have been attempting to regulate the collection, use, storage and dissemination of *personal* information. In recognition of the power of new information and communication technologies in the hands of large public and private agencies, states began to pass information privacy, or data protection, statutes designed to give individuals greater control over the information collected about them, and to stem the erosion of personal privacy (Flaherty, 1989; Bennett, 1992). The paper proceeds from the assumption that political scientists need to pay closer attention to the regulation of what, after all, is likely to be a major "currency" of the contemporary capitalist organization engaged in electronic commerce – personal information.

With the rise of the transnational corporation, employing private and public international networks, the privacy problem soon assumed an inescapably international dimension. The enforceability of information privacy laws is obviously undermined if organizations can instantaneously transmit those data to other jurisdictions for processing to escape strict regulatory responsibilities. In an era of global electronic commerce, privacy protection policies assume a central place in debates over the structure of the international political economy. The globalization thesis would thus predict two processes: first one of *policy convergence*, and second one of *policy dilution*. In other words, the ease by which a transnational corporation can transmit personal data to other jurisdictions via private and public communications networks would hypothetically lead to a harmonization of privacy standards according to the "lowest common denominator."

These questions could be addressed at a more abstract and policy level, but in order to gain a better purchase on the nature and scope of the regulatory problem, I instead present a case study of one obviously transnational industrial sector, that of the international airline system. This largely descriptive section is offered in response to a concern that comparative and international political scientists rarely study the actual practices of transnational corporations. This case study will bring into focus the extent and scope of the regulatory problem. It is drawn from a larger report just published under contract with the European Commission, which studied the transfer of five types of personal information from Europe to six other jurisdictions, which tried to assess the

"adequacy" of protection afforded in each, and which offered some lessons about the most appropriate methodology for making these evaluations.[2]

The focus will then shift to the principal instrument for transnational policy harmonization, the Data Protection Directive from the European Union, passed in October 1995, and which came fully into force in October 1998 (EU, 1995). This instrument has set the agenda for the analysis of the privacy issue by Canada, the United States and by other non-European industrialised countries. The paper concludes by evaluating the level of convergence, and the extent of policy dilution. Is the global information economy producing a "trading-up" or a "dumbing down" of privacy standards?

What happens when you book an airline ticket?

The airline industry is, of course, heavily regulated to protect customer safety, to promote environmental quality, to establish fair pricing structures and so on. An international regime has developed since the war to govern jurisdictional issues, technical interconnection, and damage control (Zacher & Sutton, 1996). There is also a healthy debate about the extent to which the industry is globalized. Some contend that airlines still remain dependent on their governments for their commercial opportunities, for subsidization, and for their national identities. Despite recent liberalization, their freedoms are significantly circumscribed by national regulatory constraints on the environment, on workforce protection, on airport planning and so on (Kassim, 1997).

However, the airline industry has rarely been a subject of concern, either by policy makers or policy analysts, for its role as a collector and processor of the personal information collected on the roughly one billion passengers carried each year. Some of this information can, however, be very sensitive. Airlines may collect a variety of medical information: on physical handicaps, diabetic status, allergic reactions, and so on. Some passengers have special dietary needs: kosher meals, no salt, vegetarian, etc., which give clues to religious affiliation or medical conditions. International airlines might receive sensitive information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parental-custody dispute), and members of groups who have certain sensitive affiliations, such as some political movements. Even more prosaic data on an individual's flying preferences has, of course, enormous commercial value for the entire direct-marketing industry.

---

[2] *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer.* European Commission Tender No. XV/97/18/D (September 1998). Besides airline reservations, the report examined electronic commerce, subcontracted outsourcing, medical data and human resources records: http://europa.eu.int/comm/dg15/en/media/dataprot/studies/adequat.pdf. Besides Canada, we studied the United States, Australia, New Zealand, Hong Kong and Japan.
I am indebted to my co-authors, Charles Raab, Nigel Waters and Robert Gellman for this stimulating research experience, which has directly influenced the ideas in this paper.

The following case study sketches the kinds of personal information that might be collected and processed when a typical traveler takes an international flight via an international carrier, from Europe to Canada, with an onward domestic flight within this country via a Canadian airline. Let us say that our traveler is a member of this airline's frequent flyer club. The case study is based on research into the practices of one typical international carrier, whose identity must remain anonymous throughout the following narrative; it will be referred to as "TRANSGLOBE AIRLINES" (TA).

The Reservation Process

Airline flights can be reserved in one of four ways: first, directly from TA's own reservation system; second through a travel agent who will have access to international reservation systems such as "Galileo" [3] or "Sabre" [4]; third, through the toll-free number associated with the airline's frequent flyer programme; and fourthly, and to an increasing extent, over the Internet. The origin of the booking does have some subtle implications for how personal data are stored and transmitted.

When the passenger books his flight, a ' Passenger Name Record' (PNR) is created in TA's Computerised Reservation System (CRS), the database for which is located at its headquarters in Europe. PNRs must contain a name, itinerary, phone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who phoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. In some cases, the PNR may also hold requests for special dietary or medical needs, all of which are accessible by internationally recognised codes which have been issued by the International Air Traffic Authority (IATA). Other codes entered on a one-off basis in these fields of the database would indicate such additional characteristics as unaccompanied minor, deportee, prisoner under escort, etc., or special needs for passengers who are not Club members.

The PNR is held on TA's mainframe computer, to which authorised TA personnel around the world have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure Control System (DCS). DCS is a subsidiary database held at TA's headquarters but, like the CRS, is accessible worldwide. The day

[3] The Galileo International system was established in 1993 and connects more than 39,600 travel agency locations to more than 530 airlines and 41 car rental companies, and all the major hotel chains and cruise lines throughout the world. The company provides travel agencies, as well as other subscribers, with the ability to access schedule and fare information, book reservations and issue tickets for more than 530 airlines. Galileo International also provides subscribers with information and booking capabilities covering all the major hotel chains, car rental companies, cruise lines and numerous tour operators throughout the world. They are headquartered in Rosemont, Illinois, and have a presence in 104 countries. Galileo supplies information and systems support to travel agencies operating more than 160,500 computer terminals, all of which are linked to the company's Data Center. The Data Center is one of the world's largest commercial data processing complexes, processing 195 million requests for information per day. See: www.galileo.com

[4] The Sabre system was originally developed by American Airlines in the 1950s. It has a similar purpose, scope and structure to those of Galileo. See: www.travel.sabre.com

before the flight, the check-in agents will ' edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated.

Most of the information recorded by TA in a PNR is either provided by or on behalf of the passenger, or is generated by TA (e.g., the flight and seat numbers). The only information obtained from third parties would be authorisations for credit-card debits and the reference numbers returned from the CRSs of any other carriers involved in the journey.

The TA ' Conditions of Carriage' declares that:

> 'The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

None of the PNR data, however, is encrypted. TA' s CRS, the DCS and the Customer and Marketing database are password-protected for all users - its own staff and check-in agents. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Europe and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS.

Checking-In and Flying

When the passenger checks in for the flight, the TA check-in staff would enter his last name to access his record on the DCS. Check-in staff (whether employees or agents) can also access this information by seat number. At a pre-set time before departure (approximately 30 minutes) a complete list of passengers by seat number is printed and given to the cabin crew; any subsequent last minute changes are notified separately. The records for each flight are purged from the DCS some two hours after the flight has landed. Printed copies of all flight lists are held at the airport of origin for 12 months. The PNR itself is purged from the CRS between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database in Europe for two years for the purpose of management analysis.

On international flights, passengers are then asked to fill in immigration landing cards, such as the ' Welcome to Canada' card issued by Canada Customs and Immigration. Passengers coming to Canada are required to provide the following information: name, permanent address, date and place of birth, nationality, passport number, flight number, purpose of visit and the value of all goods being brought to Canada as gifts. On arrival,

the passenger will surrender this card to Canada Customs which, some weeks later, will be processed and entered into the Canada Customs information system. Airline personnel will not have access to the information provided on these cards, although it may be shared and matched with data from other federal agencies.[5]

If a passenger is taking an ongoing flight with a domestic carrier, the onward flight appears as a TA-coded flight on the passenger's ticket. The details transferred would only be the relevant stage booking, the immediately-prior connecting flight and any special needs. 'Second' carriers do not have direct access to TA's CRS and do not need, or receive, the complete journey details, booking contacts or PNR history.

TA employees in Canada will have been made aware through training, and through a notice in the computer-access applications of the general policy about the disclosure of reservations information. They are reminded that: 'The carriage by air of passengers is a matter of private contract between the airline and the passenger concerned. As a general rule details of that contract should not be given to third parties particularly when the request is made on the telephone.' Employees are told not to disclose information about a passenger, including via the telephone, unless the information is given to:

- a colleague/another airline or agent for the purpose of reservation booking or ticket issue;
- the passenger himself and you have taken the necessary steps to ensure that this person is the passenger;
- some other person and the passenger has clearly consented to this and there is a record of this in the PNR;
- an appropriate person or organisation in an emergency to prevent injury or damage to someone's health.

Employees are also advised orally that requests from the police or law-enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department. They are also advised that details of medical conditions must not be disclosed without reference to the Senior Medical Officer. TA employees are also advised to refrain from placing into the central database 'any information or statement about a passenger which may be inaccurate or disparaging or discredit the passenger in any way.'

TA personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. In a telephone-sales context, they are quite strictly adhered to. If the person to whom the sales agent is speaking is not travelling, or is not mentioned in the contact field of the booking (such as the name of the secretary), then details cannot be given out. In the airport environment, however, practices may differ. TA staff and agents will have access to PNRs before, during and after a flight. A greater variety of more urgent requests arise within the airport context, in which such requests might come from

[5] The Federal Privacy Commissioner is currently challenging the constitutionality under the search and seizure provisions of the *Canadian Charter of Rights and Freedoms* of a data matching arrangement between Canada Customs and Human Resources Development Canada (HRDC) for the comparison of these customs data with unemployment insurance records. At issue is HRDC's practice of collecting data from the Customs declarations of every returning traveler to identify employment insurance claimants (supposedly available for work) who were out of the country while receiving benefits.

local law-enforcement authorities (who have jurisdiction over most airports), from the federal Royal Canadian Mounted Police (RCMP), or from Customs and Immigration officials. Working within a closer environment, personal contacts obviously develop between individuals from different authorities. TA representatives acknowledge that these personal relationships can often override the formal written guidance.

The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data will not be available in Canada (and therefore potentially open to misuse or third-party requests) for any length of time. If there are special requests from third parties after the PNR has been archived, they would have to be made in writing and considered at the European headquarters.

Frequent Flying

Recall also that the passenger is a member of TA's Frequent Flyer Club. This database holds a more complete profile of the passenger's flight history, hotel reservation and car-hire needs, frequent-flyer history, and other information. TA personnel have complete access to these data to provide the ' personalised' service that such customers have come to expect. It should be noted, however, that TA retains a separate database of its frequent-flyer passengers (including those receiving special services) in each country or region. Most other airlines retain central databases. Thus, the Canadian database on TA's frequent flyers, held in Toronto and managed by a United States marketing company, will only have information on Canadian members. It is unlikely that data on a European passenger would find its way to this database.

The application form for the TA frequent-flyer programme is presumably quite standard. The Canadian version states: ' The information requested on this application, together with the records we will retain relating to your air travel and participation...are to help us better serve your needs. This information is kept confidential at our TA Service Centre but may be disclosed to partners or other companies who provide benefits and services to TA members. Please check if: a) You do not wish the above personal information disclosed to partners or other companies; and b) You do not wish to receive separate communications about new services and facilities developed by TA and its partners.'

International Airlines as Surveillance Systems

.

Nothing in the preceding account should suggest that TA, or other major international carriers, are grossly irresponsible, or are, through conscious design constructing an onerous surveillance system. On the contrary, TA's employees, agents and sub-contractors in Canada are given exactly the same guidance about personal-information practices as their counterparts in Europe. Written policies, already cited, are disseminated in paper format and online, and security personnel assume broad responsibility for monitoring access to the central reservation system. Because it is subject to the European data protection law, TA is accountable for its personal information handling practices to the data protection authority there, which has a range of powers to ensure compliance if breaches of privacy or

weaknesses in an organisation' s systems are brought to its attention. TA also has an internal complaints-handling process, even though complaints about breaches of the privacy principles are rare.

TA is a member of the Canadian Marketing Association (CMA), and is therefore expected to comply with the CMA's code of practice when it uses passenger information for marketing purposes.[6] All airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is coordinated by the International Civil Aviation Authority (ICAO), a United Nations-affiliated body located in Montreal.[7] Airlines are subject to the 1996 ICAO ' Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS)' . Article 11 states that ' air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in the CRS' s to which they have access, and may not release such data without the consent of the passenger.' The ICAO issues standards and recommended practices for both airlines and members states, but it has no enforcement powers.

The organizational system sketched above reflects, however, the fact that international airlines have considerable power over individuals through the personal information that they collect, process and disseminate during the now routine process of undertaking international airline travel. The international airline transportation system can therefore work as a tool for surveillance. This system has the following characteristics.

First, it is *globalized.* Personal information within this system knows neither national nor organizational borders. It may find its way into reservations databases, frequent flyer databases, and into the systems of a range of local and national law enforcement organizations. Some of that information might be highly sensitive.[8]

Second, the uses or personal information have grown in an unplanned and *incremental* manner. Personal data processing practices have evolved in response to demands for greater efficiency at all stages of the process. Those demands have originated from consumers, as well as from international and national governmental agencies. The result is a largely unplanned set of personal information systems, all of which can be justified in pragmatic terms.

A third and related characteristic of this system is that it is largely *non-transparent*. In some measure this obscurity is explained by the incredible complexity of the system. In others, the lack of awareness is attributable to a relative lack of attention

[6] The CMA's privacy code can be found at: www.cdma.org

[7] www.icao.int

[8] An early indication of the kind regulatory problems that might arise under these conditions is the effort by the Swedish data protection authorities to remove sensitive data on Swedish citizens from the 'Galileo" database.

to the airlines' personal information practices by regulators, such as the Federal Aviation Authority (FAA) in the United States.

A final characteristic concerns the *contingent* nature of the information practices within this industry. It is impossible to describe definitively how personal information on any one passenger might be processed and employed. So much depends on contingent factors concerning the traveler's needs and preferences, local rules and laws, the informal industry practices, and the international conditions during travel.[9] Practices are governed, therefore, as much by informal norms as by national or international legal requirements.

The international airline system supports the larger theoretical point that the potential surveillance and power relations do not stem from the technology itself, nor from any bureaucratic imperative. The system operates in its own right as a disciplinary mechanism, in which individuals, before, during and after their travel, are constructed as manipulable entries in remote databases. Foucault (1979) utilized the metaphor of the "panopticon" to emphasise the all-seeing, routine, automatic and self-perpetuating nature of contemporary surveillance mechanisms. Power diffuses through the "capillaries" of the system. The monitoring of individual behaviour may not, at any one time, be occurring, but individuals would be well advised to behave as if it were.

A very recent example of the panoptic quality of an airlines personal information systems concerns some new rules proposed by the FAA for increasing airline security. These rules would require that all airlines conduct computerized profiling of all passengers on domestic US flights. Prompted by recent airline tragedies, the new program, called Computer Assisted Passenger Screening (CAPS), would use data from airline computers and secret profiling standards to select passengers for additional questioning and searches. Under the new rules, airlines would select passengers for increased scrutiny based on internal profiling standards. They would also randomly select some passengers for investigation for the "deterrent value that would increase airline passenger safety." The FAA funded the program, paying the carriers over $10 million to develop CAPS. The rules are based on the recommendations of the White House Commissioner on Aviation Safety and Security, led by Vice President Gore.[10] It would not be beyond the reach of the airlines' technological and administrative potential to implement such as system for international flights.

This case study of international air travel exposes, therefore, the globalized, incremental, non-transparent and highly contingent nature of personal data processing practices within this industry. There is no "Big Brother" surveillance system, here. Rather the environment has been created in a decentralized and incremental fashion as airlines have demanded, and consumers have provided, increasingly sensitive personal information. The demands for information can, for the most part, be justified as a price

[9] Spokesmen at TA confirmed that many industry practices might be altered under conditions of "heightened international tension" (such as during the 1991 Gulf War).

[10] http://www.epic.org/privacy/faa/

worth paying for more efficient and secure air travel. The practices of the airline industry are typical of those of the contemporary transnational corporation, whether in banking, insurance, information processing, the health sector and so on. They highlight, therefore, the kinds of international regulatory problems that will challenge national regulatory agencies charged with enforcing privacy rights. The discussion now turns to the European, US and Canadian approaches to this issue.

The International Regime for Personal Data Protection: "An Adequate Level of Protection"

On July 24, 1995, the Council of Ministers of the European Union formally and finally adopted a "Directive on the Protection of Personal Data with Regard to the Processing of Personal data and on the Free Movement of such Data" (EU, 1995). This approval was the culmination of five years of drafting and redrafting as the document passed through the complicated and lengthy EU decision-making process. It was agreed to by all member states with the exception of the UK (which abstained) (Bennett & Raab, 1997).

The *Data Protection Directive's* aim is to "ensure a high level of protection for the privacy of individuals in all member states...and also to help ensure the free flow of information society services in the Single Market by fostering consumer confidence and minimizing differences between the Member States' rules" (Monti, 1995). This reflects the underlying assumption that harmonized privacy protection legislation and the free flow of data are complementary rather than conflicting values, and that the single European market relies not only on the free flow of capital, goods and labour, but also of information. The hope is that "any person whose data are processed in the Community will be afforded an equivalent level of protection of his (sic) rights, in particular his right to privacy, irrespective of the Member State where the processing is carried out" (Monti, 1995).

The EU *Data Protection Directive* is a complicated instrument. It is based on the familiar set of "fair information principles," around which previous national laws and international agreements have converged (Bennett, 1992). But the text has been subject to much reworking as compromises have been struck and re-struck within the Commission, the Parliament and the Council.

The most important aspect of this Directive is its extra-territorial implications. Article 25 stipulates that "Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if...the third country in question ensures an adequate level of protection." The "adequacy" of protection shall be assessed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations." Particular consideration is to be given to the nature and purpose of the data and the "rules of law, both general and sectoral" and the "professional rules and security measures which are *complied with*" (my emphasis).

Article 26 lists a number of derogations from this provision. Personal data may be transferred to a country with "inadequate" protection when: the data subject has given his consent "unambiguously"; or the transfer is necessary to fulfil a contract between the data subject and the controller, or between the controller and a third party; or the transfer is necessary on "important public interest grounds, or for the establishment, exercise or defence of legal claims"; or the transfer is necessary to protect the "vital interests of the data subject"; or the transfer is of data that are already in a public register. Member states can also authorize transfer to a country with "inadequate" protection if the data controller enters into a contract that "adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals." In such cases, the country concerned shall inform the Commission and the other Member States of such authorizations, to allow for objections.[11]

Where the Commission decides that a third country does not ensure adequate protection, Member States are to "take the measures necessary to prevent any transfer of data of the same type to the third country in question." Then the Commission "shall enter into negotiations with a view to remedying the situation." It should be emphasized that if the Commission finds an inadequate level of protection, Member States are mandated, rather than simply permitted, to prohibit the transfer through what Schwartz (1995, p. 488) calls a "data embargo order." This represents a stronger approach than the early international instruments for data protection issued by the OECD (1981) and the Council of Europe (1981). Even though both these instruments contain a principle of "equivalence" (stronger than "adequate"), neither agreement requires their signatories to block data to countries that cannot ensure an equivalent level of protection.

The implementation of Articles 25 and 26 poses a number of problems for international businesses that rely on the transborder flows of personal data. It has major implications for credit-granting and financial institutions, for hotel reservations systems, for the direct-marketing sector (including the list rental business), for life and property insurance, for subcontracted outsourcing, as well as for the airlines. Commentators are generally agreed that the Europeans are not going to tolerate the existence of "data havens" -- jurisdictions in which data processing may take place because of the absence of data protection safeguards. The *EU Data Protection Directive* would be doomed to failure if multinationals could instantaneously transmit their processing offshore in order to avoid the transaction costs of having to abide by the stronger measures in force in Europe. European data users will be justifiably aggrieved if they have to abide by strong data protection measures in Europe, whilst overseas competitors can act with impunity. European citizens, and the public interest and consumer groups that represent them, will also not look kindly on the continual flouting of their privacy rights by overseas interests. On the implementation of Articles 25 and 26, at least, the interests of European data users, data subjects and regulators may coincide.

[11] One of the first contracts has just been negotiated by the German data protection authorities between the Germany railways and *Citibank* as a result of concerns about the development of a German Railway Card (*Bahnkarte*) and the associated processing of information about German citizens in the United States.

However, despite intense debate for around eight years, these provisions have come into force accompanied by only vague understandings about what an "adequate level of protection" means.[12] For European officials, the common assumption is that a necessary condition for such protection is a legal framework which embodies the commonly legislated data protection norms (or "fair information principles") and which is overseen by an independent supervisory authority (Bennett & Grant eds. 1999). Many multinational business interests, especially in the United States, view this position as overly restrictive and possibly inimical to technological innovation and the promotion of international electronic commerce. These differing perspectives offer an interesting background to the response in North America to the extra-territorial implications of this Directive.

"Ratcheting Up" or "Dumbing Down"?

The US Response

American policy on privacy protection is typically fragmented and incoherent. Some quite comprehensive legislation for the protection of personal data within federal, and most, state agencies is contrasted with very few legislative safeguards for data held by the private sector. With the exception of the consumer credit industry and video-rental businesses, most private corporations face no obligation to abide by the internationally recognized data protection norms. A hard-line European approach to the definition of an "adequate level of protection" could, therefore, disrupt many areas of international commerce, including the airline reservation systems.

The US attitude to the Directive has gone through a number of phases. In the early 1990s, the position of US commercial interests converged around some continuing attempts to lobby the European Commission, Parliament and Council of Ministers for more relaxed data protection standards (Regan, 1999). The business lobby consisted principally of representatives from the direct marketing, market research, consumer credit, information services, and financial industries. From the perspective of these industries, the Directive raised the real possibility that they would be forced to seek the "informed consent" of their customers before engaging in what they regard as "routine" disclosures and processing. The Directive was of particular concern to those enterprises looking to expand into the European marketplace. Some concessions were won; especially the dilution of the standard for transborder data flows from an "equivalent" to an "adequate" level of protection. However, the Directive came into force without a significant improvement in the privacy safeguards offered at the legislative level in the United States.

Other companies adopted a "let's-wait-and-see" stance and were sceptical about the willingness and ability of data protection authorities to interrupt data flows.

[12] The study cited at Fn. 2 was intended to contribute to the debate about the most appropriate assessment of "adequacy."

Moreover, if the provisions of Article 25 were to be enforced, there is an expectation that contractual arrangements can protect the interests of the large US multinational companies. The implicit belief is that there is sufficient latitude in the Directive for data users in third countries to convince their European counterparts that a combination of contracts, codes of practice and security measures can afford "adequate" data protection.

Some businesses that were to continue to rely on the uninterrupted flows of personal data from Europe to the United States also began to adopt privacy codes of practice (Privacy and American Business, 1994). In the hope that these would qualify as the kind of "professional and security measures" mentioned in Article 26 of the Directive, some businesses and trade associations hoped that *bona fide* attempts at self-regulation would preempt any regulatory intervention when the Directive came into force (in October 1998). As part of the National Information Infrastructure agenda of Vice-President Gore, a set of voluntary privacy principles have been negotiated through an Information Infrastructure Task Force (United States, IITF, 1995). Privacy codes have been a feature of this policy landscape for some time, but unless they are given legal force, they tend to be regarded with scepticism within the policy community of advocates, commissioners and experts that has coalesced around the privacy issue. They invariably suffer from the criticism that the protection of personal data is in the hands of the organization that can have the most to gain from its unregulated processing and disclosure (Bennett 1995).

More serious perhaps is the recognition of the Federal Trade Commission that action can be taken to protect privacy through existing consumer protection laws, when "unfair or deceitful" marketing is discovered and challenged. But regulatory intervention is only contemplated when there has been an "identifiable market failure" (Varney, 1996). In addition, and in response to the burgeoning economy in online retail sales, a series of efforts to develop privacy-friendly websites has also been initiated by the FTC.[13]

When October 1998 approached, therefore, a transatlantic trade war over personal data was considered a definite possibility. The more radical privacy advocates were talking of registering complaints against US multinationals whom, they believed, were not meeting the terms of the Directive. The US federal government was under increasing pressure, from business, to defend its interests not only within the EU, but also within the World Trade Organization. As a result, a series of bilateral negotiations have ensued between the US Department of Commerce and the European Commission to permit personal information to continue to flow freely to the United States under conditions that fall short of European expectations. The Americans support the position that a "safe harbour" for personal data can be successfully negotiated provided those companies that require the international flow of personal data for their continued operations adhere to an acceptable standard of self-regulation.[14] Negotiations are

[13] Examples are the Truste system: www.truste.org; the Better Business Bureau inititiative, BBBOnline: www.bbb.org , and the P3P system: www.w3.org/p3p . The FTC has been monitoring the use of privacy notices on the internet since 1997.

[14] The 'Safe Harbor Principles" are available at: http://www.ita.doc.gov/ecom/menu.htm

currently ongoing, but have also been subject to some considerable criticism from the consumer privacy lobby.[15]

Generally resistant to a comprehensive data protection statute that would cover all private organizations, regardless of size, type of business, and the sensitivity of the data they collect, the US Congress has been considering a range of sectoral privacy legislation. In the 105th Congress alone, some 150 bills were introduced on privacy-related topics. Of these, only none were passed into law, dealing with issues such as identity theft, children's privacy, the use of Social Security Numbers, and consumer credit.[16] A range of other issues (on financial services, online privacy, digital signatures, health and genetic privacy, encryption, and employee surveillance) are currently under consideration in the 106th Congress.

It is difficult to know how much of this increased activity can be attributed to the influence of the European Directive. The essential characteristics of American privacy policy have not changed; it is fragmented, incoherent and largely reactive (Gellman, 1993; Regan, 1995). A reliance on sectoral legislation where evidence of harm is clear, and self-regulation where it less clear, have been the hallmarks of US policy since the 1970s. On the other hand, privacy protection is now higher on the American policy agenda than at any time, probably since Watergate. The European Directive, and its extra-territorial implications, is clearly one important factor that explains this trend.

The Canadian Reaction

Canadian policy on privacy protection has, until recently, mirrored that of the United States. Some quite early privacy legislation covering the federal public sector (the 1982 Privacy Act) has been subsequently followed by information and privacy acts in most of the provinces. Until very recently, however, data protection in the private sector relied mainly on the implementation of certain self-regulatory codes of practice promulgated through the major trade associations in banking, insurance, telecommunications, direct-marketing and so on (Bennett, 1996).

In 1992, partly as a result of the European Data Protection Directive as well as a new private sector data protection law in Quebec,[17] the issue assumed a greater prominence within two arenas, both of which spanned the federal/provincial divide. The first is the Canadian Standards Association (CSA). From 1992 to 1995, representatives from government, industry and consumer groups negotiated a "Model Code for the Protection of Personal Information" (CSA, 1996). A committee updated and revised the *OECD Guidelines*, with reference to the new Quebec legislation and the emerging *EU*

---

[15]. The Trans Atlantic Consumer Dialogue (TACD) has recently adopted a resolution in Brussels that calls on the European Commission to reject the U.S. "Safe Harbor" proposal. TACD recommended instead the establishment of an International Convention on Privacy Protection to address public concerns about transborder data flows. The Safe Harbor proposal is deemed problematic in that it fails to provide adequate privacy protection for consumers.

[16] See, *Privacy and American Business,* Vol. 6, No. 2, February/March 1999.

[17] In 1993, Quebec passed Bill 68, *An Act respecting the protection of personal information in the private sector.* This legislation was based on the European data protection model.

Data Protection Directive. The CSA code is intended to establish common safeguards to protect personal information throughout the entire private sector. It would then be adopted by different sectors, adapted to their specific circumstances, and used as a way to promote "privacy friendly" practices.

The code was finalized and approved without dissent in September 1995. It is was then formally ratified as a "standard" by the Standards Council of Canada, and published in March 1996. The CSA has also announced a "Recognition Program" to certify industry codes and practices. There is potential to register data users (in both private and public sectors) to the standard and thus to oblige them to implement the privacy principles. The scrutiny of operational manuals and/or on-site auditing are a prerequisite for maintaining a registration to the CSA privacy standard (Bennett, 1995). In this respect this instrument represents more than the typical "voluntary code." As with other "standards," adoption of the code carries clear obligations to implement its provisions and demonstrate to an independent registration or certification authority that its provisions are being properly implemented. Registration to this code could therefore demonstrate compliance to data protection standards to overseas regulators and business. However, adoption of the code would still be voluntary even though pressures can be exerted by government, by international data protection authorities and by consumers and clients. The process of building a system of data protection in Canada would still be incremental and piecemeal (Bennett, 1995).

Partly for these reasons, the Canadian Advisory Council on the Information Highway passed a set of recommendations in 1995 to "ensure privacy protection on the Information Highway" (IHAC, 1995). In addition to encouraging the adoption of voluntary standards based on the model CSA code and the analysis of a range of technological solutions (mainly public-key encryption), the Advisory Council recommended that the federal government:

> create a level playing field for the protection of personal information on the information highway by developing and implementing flexible framework legislation for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA model code, while allowing the flexibility to determine how they will refine their own codes.

In his 1994-95 Annual Report, the Federal Privacy Commissioner suggested that the CSA privacy code be added to the federal Privacy Act, meaning that "observance of the CSA standards would become a legal obligation and would be supported by a system of independent oversight" (Privacy Commissioner of Canada, 1995, p. 7). Furthermore, the Canadian Direct Marketing Association publicly supported national privacy legislation based on the CSA standard late in 1995. The CSA process was more, therefore, than the negotiation of a voluntary code. It has become the essential stage of brokerage between data users, consumer groups and government (Bennett, 1996).

The consensus at the CSA table as well as the recommendations of the industry-dominated advisory council produced a federal government announcement in May 1996 (Industry Canada, 1996, p.25):

> As a means of encouraging business and consumer confidence in the Information Highway, the Ministers of Industry and Justice, after consultation with the provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector.

In September 1996, Justice Minister Allan Rock addressed the Annual Conference of the International Privacy and Data Protection Commissioners conference in Ottawa and clarified this commitment: "By the year 2000, we aim to have federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector." The Minister cited the European Directive and assured his audience that "we are aware of how the approaching deadline of 1998 will affect the transfer of personal data from the Union's member countries" (Rock, 1996).

In October 1998, therefore, the Federal Government introduced Bill C-54, "The Personal Information Protection and Electronic Documents Act," which is currently making its way through the House of Commons. This bill applies the data protection principles articulated in the CSA Model Code to the federally regulated private sector, and to any other business that transmits personal data inter-provincially and internationally for commercial reasons. Relying on its trade and commerce powers, the federal government is attempting to brand Canada as a truly safe jurisdiction in which personal data might be processed, in implicit contrast to the United States. More controversially, the Government has also stated that Bill C-54 will apply to those businesses normally regulated under the provincial jurisdiction unless "substantially similar" legislation is passed within the provinces within three years.[18]

Conclusion: Globalization, Surveillance and the Regulation of International Networks

The reasons for a legislative approach in Canada, in contrast to that of its major trading partner, have been addressed in other writings (Bennett, 1996; Bennett & Raab, 1997). Certainly the impact of Quebec's legislation in Canada is a significant difference. Moreover the structure of trade associations, more inclusive in Canada means that the reputations of members of organizations such as the Canadian Marketing Association can be more easily harmed by the non-compliance of free-riders.

Despite the continuing differences between Canadian and US privacy protection policy, however, it is fair to say that privacy protection has never assumed a higher

[18] The relevant documents relating to Bill C-54 can be found at: http://e-com.ic.gc.ca/english/pivacy/632d1.htm

importance on the national agendas of both countries.[19] Certainly the arrival of the Internet and its use for online commercial activity is a major force behind this increased concern for personal privacy: consumers need the confidence that their personal information (such as credit card numbers) is being handled confidentially. But the impact of the international agreements (from the OECD, the Council of Europe, and most notably the European Union) has been very significant. The EU Directive has established the rules of the road for the increasingly global character of data processing operations (Reidenberg, 1993).

In terms of the globalization thesis, therefore, this case demonstrates that indeed there has been a high level of policy convergence. Over time, these international harmonization efforts, as well as an increasing cross-fertilization of policy ideas have motivated a considerable consensus (at least among the industrialized countries) about what it means for an organization to pursue privacy-friendly practices. These fair information principles now appear in around 30 national laws, in international agreements, in voluntary codes of conduct, in the CSA's model privacy code, and (with some variations) in the "Safe Harbour Principles" being negotiated between the US and Europe (Bennett & Grant, 1999, p. 6). The European Directive, with its insistence that data protection laws should be overseen by a "supervisory authority" is also beginning a process of convergence not only around the statutory principles, but also around the policy instruments through which those principles should be enforced (Bennett, 1997). The United States currently resists the establishment of a privacy protection agency or Commissioner. Most other countries (including New Zealand, Hong Kong, Australia and Canada) have accepted the need for an independent privacy watchdog.

What is clearly not observed in this case is a process of policy dilution. So far, the convergence dynamic has operated to harmonize data protection rules to the highest, rather than the lowest, common denominator. That standard is embodied within the European Union's Data Protection Directive. This process approximates what David Vogel has described as "trading up" in his analysis of the impact of trade on environmental and consumer product regulation (Vogel, 1995). More specifically, Vogel has described a "California Effect" to denote the "ratcheting upward of regulatory standards in competing political jurisdictions." The pattern is driven by three separate influences: 1) where stricter regulations represent a source of competitive advantage for domestic firms and the latter then support them in the international arena; 2) where the nations which have enacted stronger standards force foreign producers to adjust to those standards in order to continue to enjoy market access; and 3) where agreements to reduce trade barriers can provide the pioneers with the opportunity to pressure other countries to adopt those stricter standards (Vogel, 1995, pp. 259-260).

Each of these processes is observed in the data protection case. There is an obvious wish to use privacy protection for competitive advantage, as is witnessed by the increasing tendency of businesses in North America to adopt voluntary codes of practice,

[19] See for example, the cover story in the May 1st-7th, 1999 edition of *The Economist,* "The End of Privacy."

and to publicize these self-regulatory efforts through publicity brochures.[20] Secondly, the European data protection laws (harmonized through the Data Protection Directive) have forced transnational corporations to abide by these regulations when they do business in Europe. The transaction costs for harmonizing global information systems to these higher standards may be less than those of operating different systems according to different standards in different countries. This "ratcheting-up" is clearly observed in the case of TA, and the other international carriers that have to operate in Europe. If the airline has to process personal data on European citizens according to the European laws, then how can it separate non-European customers in its databases for processing to a lower standard? And thirdly, we also see a considerable effort to pressure those without comprehensive privacy protection laws to adopt them. This pressure has stemmed from officials within the European Commission, as well as from certain influential data protection commissioners, who after all now have the power to disrupt the international trade in personal information.

One other feature of this case deserves comment. Historically, it has been non-Americans who have been concerned about the extra-territorial impact of US domestic policy. The "hegemonic" position of the United States in the international economy has typically created "externalities" requiring a range of policy responses in economic, trade, environmental and other areas. In the area of human rights, there is also a perception that influence has historically flowed from the United States to Europe. The reversal of this pattern has not gone unnoticed. As George Trubow remarks: "It will be ironic, indeed, if Europe's insistence on the protection of human rights causes this country to pay some real attention to informational privacy in both the public and private sectors. Usually we are in the position of lecturing other nations about the sanctity of fundamental human rights; in the informational privacy dimension we are the ones who must be lectured" (Trubow, 1992, p. 175). Alan Westin comments that "we deliberately chose to break with European institutions in 1776, and it would be remarkable if we thought that a return to deference without agreement was the right course in 1996" (Westin, 1996).

A final reservation is, however, in order. These judgements apply to the countries of the advanced industrial world. For very few countries outside of the OECD has privacy protection been a salient issue. The test of the international data protection regime, administered through the Directive, may not be the extent to which a trade war with the US can be avoided, but whether or not this regime can prevent the processing of personal data in the lower wage economies of the developing world. A truly global solution to this problem will require, therefore, more than legislation and regulatory oversight. It is now realised that only a range of approaches, including privacy-enhancing technologies, market inducements, and certifiable privacy standards, will promote a ratcheting–up of organizational practices, as well as a trading up of national policies (Bennett & Grant, 1999).

[20] A good example would be the leaflets that one can now pick up in any Canadian bank about one's right to financial privacy. In the online world, IBM has recently announced that it will not advertise on websites that do not display a prominent privacy statement.

REFERENCES

Beniger, J.R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, Massachusetts: Harvard University Press.

Bennett, C. J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Ithaca, NY: Cornell University Press.

_____. 1995. *Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association.* Rexdale: Canadian Standards Association, PLUS 8830.

_____. 1996. Rules of the Road and Level-Playing Fields: The Politics of Data Protection in the Canadian Private Sector. *International Review of Administrative Sciences* 62: 479-92.

_____.1997. "Convergence Revisited: Toward a Global Policy for the Protection of Data?" In Philip E. Agre and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge Massachusetts: The MIT Press.

Bennett, C.J. & Grant, R. 1999. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press.

Bennett, C.J. & Raab, C.D. 1997. "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response". *The Information Society*. Vol. 13, pp. 245-63.

Canadian Standards Association (CSA). 1996. *Model Code for the Protection of Personal Information*. CAN/CSA-Q830-96. Rexdale: CSA. (http://www.csa.ca)

Castells, M. 1996. *The Rise of the Network Society*. Oxford: Blackwell Publishers.

Council of Europe. 1981. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Strasbourg: Council of Europe.

European Union. 1995. *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.* Brussels: OJ No. L281. 24 October 1995. (The EU Data Protection Directive)

Flaherty, D. H. 1989. *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.

Foucault, M. 1979. "Panopticism". *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Gellman, R. M. 1993. Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions. *Software Law Journal* VI: 199-238.

Gill, S. 1995. "Globalisation, Market Civilisation, and Disciplinary Neoliberalism". *Millennium: Journal of International Studies*. Vol. 24, No. 3, pp.399-423.

Hirst, P. 1997. "The Global Economy - Myths and Realities". *International Affairs*. Vol. 73. No. 3. July 1997. Pp. 409-25.

Industry Canada. 1996. *Building the Information Society: Moving Canada into the 21st Century.* Ottawa: Industry Canada. (http://info.ic.gc.ca/info-highway/ih.html)

Information Highway Advisory Council (IHAC). 1995. *Connection, Community, Content: The Challenge of the Information Highway.* Ottawa: Minister of Supply and Services Canada. (http://info.ic.gc.ca/info-highway/ih.html)

Kassim, H. 1997. "Air Transport and Globalization: A Sceptical View". In Scott, A. *The Limits of Globalization*. New York: Routledge.

Monti, M. 1995. *Council Definitively Adopts Directive on Protection of Personal Data*. European Commission Press Release, IP/95/822, July 25, 1995.

Negroponte, N. 1995. *Being Digital.* New York: Knopf.

Ohmae, K. 1990. *The Borderless World: Power and Strategy in the Interlinked Economy*. New York: HarperBusiness.

Organization for Economic Cooperation and Development (OECD). 1981. *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*. Paris: OECD.

Perraton, J. Goldblatt, Held, & McGrew. 1997. "The Globalisation of Economic Activity". *New Political Economy*. Vol. 2, No. 2. July 1997.

Privacy Commissioner of Canada. 1995. *Annual Report 1994-95*. Ottawa: Canada Communications Group.

Privacy and American Business. 1994. *Handbook of Company Privacy Codes.* Hackensack NJ: Privacy and American Business.

Raab, C. D. Bennett, C. J. Gellman, R. N.Waters. 1998. *Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer.* European Commission Tender No. XV/97/18/D (September 1998)

Regan, P. M. 1995. *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina Press.

_____. 1999. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics." In Bennett and Grant eds. *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press).

Reidenberg, J. R. 1993. Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms. *Harvard Journal of Law and Technology* 6: 287-305.

Rock. A. 1996. Address to the Eighteenth International Conference on Privacy and Data Protection. Ottawa: Department of Justice.

Schwartz, P. M. 1995. European Data Protection Law and Restrictions on International Data Flows. *Iowa Law Review* 80 (3): 471-96.

Schwartz, P.M & J. M. Reidenberg. 1996. *Data Privacy Law: A Study of United States Data Protection.* Charlottesville, VA: Michie.

Strange, S. 1996. *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge: Cambridge University Press.

Toffler, An. 1980. *The Third Wave*. New York: Bantam Books.

Trubow, G. B. 1992. The European Harmonization of Data Protection Laws Threatens U.S. Participation in Trans Border Data Flow. *Northwestern Journal of International Law and Business* 13 (1): 159-176.

United States Information Infrastructure Task Force (IITF). 1995. *Privacy and the National Information Infrastructure: principles for Providing and Using Personal Information*, Final Version, June 6. Washington DC: IITF, Information Policy Committee, Privacy Working Group.

Varney, C. 1996. Consumer Privacy in the Information Age: A View from United States FTC. *Privacy Laws and Business* 36: 2-7.

Vogel, D. 1995. *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Cambridge, Massachusetts: Harvard University Press.

Weiss, L. "Globalization and the Myth of the Powerless State". *New Left Review*. Vol. 225, No. 3, Sept/Oct 97.

Westin, A.F. 1996. Testimony before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, U.S. House of Representatives, Washington D.C. June 11, 1996.