Transboundary Challenges to Privacy Protection[1]

Stephanie Perrin

August 2015

This report examines briefly the history of trans-border dataflow debates in the context of the protection of personal data, bringing us up to the current environment of "cloud" services and increasing global enthusiasm for "big data". It is often stated in the public press that privacy law and policy are outdated, that no one could have anticipated this global, dynamic traffic of personal data. I contend the contrary, that far-sighted anticipation of increasing dataflow and loss of user control have been at the heart of data protection discussion for the past half century. In fact, we may have been more honest about the challenges when there was less data protection law that purported to deal with the issue.

Many barriers interfere with implementation of data protection, not the least being getting laws enacted in this new and evolving field. Another problem has been the scarcity of resources and focus placed on finding effective mechanisms that allow individuals to enforce their basic human right of exercising control of their own data. Accompanying this practical problem is the political pressure to compromise, where economic and national security interests demand a different

[1] Stephanie Perrin, "Transboundary Challenges to Privacy Protection," August 2015. This report was prepared as part of a research project funded by the Office of the Privacy Commissioner of Canada's 2014-2015 Contributions program: "Assessing the Privacy Risks of Extra-National Outsourcing of eCommunications" and forms Appendix E of the final report. The complete project findings and recommendations are available at http://ecommoutsourcing.ischool.utoronto.ca/. This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author and do not necessarily reflect those of the OPC.

balancing of individual vs. institutional rights. Finally of course, the complexity of extra-jurisdictional enforcement of law complicates trans-boundary privacy protection, especially where some fundamental rights are assured by constitutional law in some but not in all jurisdictions. Some constitutional rights protect all people, many only protect citizens and residents of the particular state.

Some argue that most personal dataflow does not appear to result in significant harm to other human rights of individuals, but in the age of big data, this is difficult to verify[2]. In any case, the lack of evidence of harm for the majority does not excuse the growing disregard for the rights of those for whom trans-border dataflow does or could cause harm. It is becoming an increasingly unrealistic assertion, as we start to see the damage that can accrue to individuals from data breaches, criminal penetration of institutions, and changes of regime which put the rights of individuals to freedom of political, religious, and sexual expression in jeopardy. Even old data can become a new threat when placed in hostile hands.

This article examines the history of attempts to harness trans-border dataflows, the experience of best practice codes and self-regulation, and the calls for international coordination. In the last section, I looked at the current problems associated with dynamic dataflow and the cloud computing phenomenon, and the prospects for transboundary enforcement of data protection and human rights, particularly in the context of Internet governance. In this context, I examine the current privacy issues at ICANN, the Internet Corporation for Assigned Names and

[2] http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

Numbers, where a debate over privacy interests in the WHOIS global public registry of domain name registrants has gone on for a decade and a half.

Transborder dataflow or TBDF was a major driver for the development of data protection law during the 1970s, as nations realized that there were economic benefits in sending data offshore for processing, particularly in the financial industry. In Canada, a report prepared by the federal task force on privacy and computers in 1972[3] declared that already, much of the sensitive data of Canadians was stored in databanks in the United States. At the time, Canada did not have a privacy statute, but at least in the view of the drafters of the report, the United States had some sectoral regulation to protect the data which was flowing into the US as a result of the data processing industry. Therefore, the major concern regarding TBDF which the task force cited was loss of control of the sovereignty of citizen data (p. 171). The report offered four suggestions to deal with the problem of extra-territorial control of personal information: rely on existing US law for protection; require companies exporting data to register with an authority in Canada; require the latter but also keep a duplicate copy in Canada; and fourthly, insist that data stay in Canada (p.171-172). Remembering that this was 43 years ago, prior to the Internet, it is interesting that the recommendations sound similar to the options discussed today. In the wake of the Snowden revelations concerning widespread data surveillance, many countries are expressing concern about the extent to which their sensitive data is held outside the country, and intercepted for

[3] Department of Communications and Department of Justice, (1972). *Privacy and Computers*. Information Canada, Ottawa.

intelligence purposes.[4] Some are calling for controls to keep personal data within the country or region, leading to concern that such controls will lead to a "balkanization" of the Internet.

Canada was not the only country studying the intersection of privacy and computers during the 1960s. It was not until the next decade that the trans-border flow of personal data became the subject of exhaustive study and meaningful response. The Organization for Economic Cooperation and Development (OECD) struck a committee in 1978 to draft the Guidelines for the Protection of Personal Information and Transborder Dataflow, which appeared in 1980. Meanwhile, the Council of Europe adopted two resolutions on data protection: Resolution (73) 22 established principles of data protection for the private sector and Resolution (74) 29 did the same for the public sector.[5] The Council of Europe released Convention 108 in 1981, calling for countries to harmonize their data protection laws by signing onto the Convention and to focus on cooperation.

Both the OECD Guidelines and Convention 108 went on to become the basis for much data protection law, but the recommendations for further study of the regulation of trans-border dataflow and international cooperation did not receive as much attention, and appeared to stall during the 1980s. For the OECD Guidelines, it is noteworthy that the explanatory memorandum stressed efforts to cooperate across borders, but the memorandum itself was much less widely disseminated and

[4] *New EU rules to curb transfer of data to US after Edward Snowden revelations*, October 1, 2013, The Guardian, http://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden.
[5] See the Explanatory Report of *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), http://www.conventions.coe.int/Treaty/EN/Reports/HTML/108.htm

read. In Convention 108, Chapter 3 deals with transborder dataflow requirements, and Chapter 4 deals extensively with mutual assistance in assuring rights of citizens outside the home country, along with the detailed requirements to name competent authorities. Signatories to the Convention were obliged to enact data protection legislation, whereas those who endorsed the OECD Guidelines had no such obligations. Nevertheless, by 1990 it was apparent that the Convention was not producing results as quickly as required within the growing European common market, and the European Commission started work on the draft Directive 95/46[6]. Throughout this period, several scholars called for further attention to the issue of TBDF, but the speed at which new innovations in technology were bringing privacy issues to the fore meant that extra-jurisdictional issues were not always the principle focus. Just to name a few privacy challenges, it was during this period that the personal computer hit the desktop, the telephone signaling system changed, permitting Calling Number Identification or Caller-ID, the cell phone was launched, video surveillance cameras became popular, and of course in the 1990s the Internet and e-mail became a commercial reality. Data protection authorities – still new at this time and not found in many jurisdictions - had a hard time keeping up. Getting privacy law into place was a primary concern. When the draft European Directive on data protection was tabled in 1990[7], there was a twin focus: the necessity to enact law that was at least congruent in its aims and requirements, and the

[6] Directive (EC) 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L.281/31, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[7] Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 oJ. (C 277) 3.

obligation to control trans-border dataflow by restricting the flow of personal data to jurisdictions that did not have "equivalent" data protection law.

The draft directive contained a clause that restricted the transfer of data to countries which did not have "equivalent" data protection, prompting great concern in the United States and among global business interests. Eventually this language was changed to "adequate", after considerable negotiation. Although the struggle over the directive was primarily fought out in Brussels and at the different fora where data protection issues were discussed (eg. the OECD, the annual Data Protection Commissioners' Conference) the issue of TBDF was of huge importance and influenced the GATT negotiations over trade in telecom services, the North American Free Trade Agreement, and others. The struggle over the data export provision in the Directive is often described as reflecting a fundamental difference in the way Europe and the United States see data protection. In Europe data protection is a human right, whereas in the US it is regarded as a management practice, to be assessed and regulated (if at all) on a sectoral basis. In an early article on the need for international standards, however, Professor Spiro Simitis, who was the first Data Protection Commissioner of the State of Hesse in 1970, canvasses a wide range of legal precedents and constitutional cases in Europe and in the US, and discusses in depth why this notion is not true. He concludes with a warning:

> The processing of personal data is not unique to a particular society. On the contrary, the attractiveness of information technology transcends political boundaries, particularly because of the opportunity to guide the individual's behavior. For a democratic society, however, the risks are high: labeling of individuals, manipulative tendencies, magnification of errors, and strengthening of social control threaten the very fabric of democracy. Yet,

> despite the incontestable importance of its technical aspects, informatization, like industrialization, is primarily a political and social challenge. When the relationship between information processing and democracy is understood, it becomes clear that the protection of privacy is the price necessary to secure the individual's ability to communicate and participate. Regulations that create precisely specified conditions for personal data processing are the decisive test for discerning whether society is aware of this price and willing to pay it. If the signs of experience are correct, this payment can be delayed no further.[8]

US privacy expert Robert Gellman, a veteran of legislative battles in the US Congress to expand privacy protections, echoed the concerns that Simitis expressed about the need to address privacy matters with international rules in 1996:

> The question presented is a simple one, although the answer is complex and uncertain. Is it possible to provide effective privacy protections on a national level, or will it be necessary to have international rules to have meaningful protections? Framed more precisely, are modern information technology and multinational business activities combining to outstrip the ability of individual countries to regulate the use of personal information about their citizens?[9]

Gellman prefaces his discussion with three caveats that have proved prophetic: firstly, the US lagged its international partners in enacting data protection law; this is even more emphatically the case in 2015 although the Federal Trade Commission has stepped up to play the role of a data commissioner in the International Conference of Data Commissioners, despite the limitations of its jurisdiction and enforcement powers. Secondly he notes that the first flush of enthusiasm in the establishment of data commissioners and their staffs is over, bringing the possibility that bureaucracy will set in and interfere with the boldness required to deal with complex problems, and thirdly, he notes

[8] Spiros Simitis, *Reviewing Privacy in an Information Society*. 135 University of Pennsylvania. Law. Review. 707 1986-1987 p. 746

[9] Robert M. Gellman, *Can privacy be regulated effectively on a national level? Thoughts on the possible need for international privacy rules.* Villanova Law Review 41 129 1996, p. 130.

> …information technology is advancing so rapidly that privacy controls may, as a practical matter, become harder to draft and to enforce. Existing policies may lose their effect as computer networks make distance and national borders irrelevant to communications, information disclosures and economic transactions. Traditional distinctions between types of records and classes of record keepers are fading. The world may have neither the will nor the ability to write privacy rules that can keep pace with the results of changing technology. (p.132)

Gellman concludes that it remains to be seen whether nation states alone can guarantee that fair information practices can protect the data of their citizens in an information society characterized by global data flows.

Gellman mentions briefly the possibility of an ISO standard, referring to a Canadian attempt to provide a solution for transborder data flow. The Canadian Standards Association (CSA) struck an experts group in 1991, to develop a model code for the protection of personal information, based on the OECD Guidelines. A multi-stakeholder committee gathered over five years, hammering out a more specific and detailed set of management practices to govern the handling of personal information, and CAN/CSA-Q830-96 was accepted as a National Standard by the Standards Council of Canada in 1996. This model code is a quality standard, which means that organizations wishing to be certified to the standard can do so as part of a quality ISO 9000 accreditation. One objective was to solve many compliance problems by facilitating neutral audit of data protection practices, particularly of contractors and subcontractors overseas, where there might not be national privacy law or data commissioners empowered to investigate data breaches. Another objective was to influence evolving security management standards, in order that

they would recognize privacy risk as a matter which needed to be assessed separately from security risks.

Canadian attempts to advance the CSA standard at ISO went on until 2000, but they were mostly unsuccessful. US companies were largely unsupportive of quality standards. Given the ongoing struggle to get European states to implement privacy legislation which met the standard of the new data protection Directive 95/46, there was little enthusiasm for the initiative in that quarter as well. The Article 29 Working Group noted the initiative positively in an opinion in 1997[10], but the timing of this initiative was probably not good, as the US was in the process of negotiating and implementing its own Safe Harbor Agreement with the EU, to permit transfer of data to the US despite their own lack of data protection law in many sectors. In the meantime, the CSA standard became the basis for the private sector legislation which passed in Canada in 2000, the *Personal Information Protection and Electronic Documents Act* or PIPEDA.[11] The fact that it was based on a standard made it easy for Canadian provinces to adapt and apply in their own jurisdictions. Various aspects of the Code, however, notably the enhanced accountability principle, have had significant impact in the global discussions of management practices to protect personal information.

It is beyond the scope of this article to discuss exhaustively all the attempts to create further incentives for the protection of personal information in the context of transborder dataflow. It remains a well-recognized problem. Christopher

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp2_en.pdf
[11] See Perrin, Black, Flaherty and Rankin, 2001. *The Personal Information and Electronic Documents Act, An Annotated Guide*. Toronto, Canada: Irwin Law.

Kuner[12] explores options to replace the "determination of adequacy" which appears in the Directive, proposing instead a focus on accountability similar to what Canada included in PIPEDA. PIPEDA insists that data controllers "shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party" (*PIPEDA,* section 4.1.3).[13] Kuner points out that the determination of adequacy is slow, cumbersome, and labour intensive, whereas the global requirement for trust in each others' data protection practices demands nimbler solutions. The Canadian solution proposed the possibility of independent audit, without which it is hard to ensure that global trust.

The next act is this continuing drama is the current renegotiation of Directive 95/46, to enact a Data Protection Regulation[14] for the European Community, that solves some of the ambiguity and uncertainty inherent in an approach where each nation state has its own data protection law. Just as Spiros Simitis described in *From the State to the Polis*[15], there were many compromises in this negotiation. Some privacy experts are hoping the European Parliament will not pass the Regulation, which would leave the 95/46 Directive in place, and the laws which meet its standard.[16]

---

[12] Kuner, C. (2009). *Developing an Adequate Legal Framework for International Data Transfers* in Reinventing Data Protection?, eds. Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., and Nouwt, S. Springer. DOI 10.1007/978-1-4020-9498-9

[13] See Perrin supra note 7 p.16 for a discussion of this clause in the context of TBDF.

[14] http://amberhawk.typepad.com/files/dapix-text-eu-council-dp-reg-december-2014.pdf

[15] Simitis, S. *From the State to the Polis*, 80 Iowa L. Rev. 445 1994-95.

[16] Pounder, C. (2015). Hawktalk Blog, February 18, 2015, *Why the Data Protection Regulation is likely to provide a lower level protection than Directive 95/46/EC.* http://amberhawk.typepad.com/amberhawk/2015/02/why-the-data-protection-regulation-is-likely-to-provide-a-lower-level-protection-than-directive-9546.html

Where does this leave us as we examine the ongoing debate over Internet governance? As we review the articles cited above, it should not be a surprise to find technology outstripping our ability to legislate effectively for privacy. Some anticipated these difficulties for decades. Steadily, the economic drivers for transborder dataflow and for the untrammeled use of personal information continue to grow, and the current emphasis on a risk-based approach to privacy protection (as opposed to a rights-based approach) suggests that data protection may be straying from its original goals. The high Courts are still capable of pushing data protection back to its original track, but it may take time and the ultimate result is not yet clear and may never be clear.

In the meantime, the enthusiasm for "cloud computing" means that it is increasingly difficult to locate where personal data resides at any given instant. The data is definitely somewhere in a computer or server located in a discrete location, even if that location is subject to change at any time. Under most existing data protection rules, data controllers must take responsibility for every device they use to hold personal data, and they must be able to tell the data subject where it is, and respond effectively to requests to access, correct, and delete the data...everywhere it is. That is the law, at least, in many but not all jurisdictions. The extent to which data controllers actually comply with those laws is beyond the scope of this effort to describe other than to say that compliance cannot always be assumed.

The still inchoate "right to be forgotten" recently came into sharper focus with respect to Internet search engines[17]. In May 2014, the European Court of Justice (ECJ) issued its decision in the Google Spain case.[18] A Spanish citizen, finding in 2010 that the results of a Google search of his name included a 1998 newspaper article detailing an embarrassing debt situation and the resulting forced sale of his property, complained to the newspaper and to Google. Given that it was 10 years later and he had resolved the financial issues, he felt that the link should not still be available. When the two companies refused his request, he complained to the Spanish data protection authority (AEPD). The AEPD investigated, and ordered Google to remove the links. Google then challenged the ruling, which eventually brought the case to the European Court of Justice.

The Court found that the operator of a search engine does indeed collect, retrieve, disclose and store information just like other data controllers, and therefore is under the same obligations. Therefore, the Court held that Google had an obligation to remove the data, as a data controller. The Court recognized that under certain situations removal would not be appropriate, and that the individual's rights of informational self-determination must be balanced against the interests of the public in having access to information. Furthermore, and importantly in this

[17] See Perrin, S., Gellman, R. and Barrigar, J. for a more detailed analysis of this case in *Government Data Sharing: Is data going out of the silos, into the mines?* An independent research report commissioned by the Information Commissioner of Alberta. http://www.oipc.ab.ca/Content_Files/Files/Publications/Report_GovtInfoSharing_Jan2015.pdf

[18] *C-131-12: Google Spain* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir&cid=437838. For the European Commission's factsheet on the case, see http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf

discussion, it raises yet again the issue of what is to be done if the data is deleted in one jurisdiction (Spain) but is accessible elsewhere (e.g., the United States).

Privacy advocates may be heartened by this recent case, but it certainly prompted controversy because of its potential impact on accessibility of information, the freedom of the press (note that neither the data protection authority nor the court told the newspaper to delete the information), and on the availability of information about miscreants, politicians, and other public figures. This tension between transparency and accountability, and the rights of individuals and organizations to confidentiality and anonymity, is not easy to regulate. This same tension lies behind the long struggle over the accessibility of the WHOIS public directory for domain names.

WHOIS is the name of the directory of the registrants of domain names on the Internet. It is not an acronym. It started out as the name the early researchers who created the Arpanet used to refer to the list of Internet addresses and domain holders. As the Internet grew and became commercial, so did WHOIS, and eventually when ICANN was formed in 1998 to manage the assignment of names and numbers, firm requirements with respect to the collection, use, and public disclosure of registrants of domain names became part of the first contractual requirements for registrars. Privacy advocates responded by demanding privacy and proxy services, whereby another organization put their information into the public directory, and registrars soon started offering these services to cloak the identity of registrants. Governments and law enforcement authorities, backed up

by copyright and trademark holders, protested that privacy/proxy services were being abused by criminals.

From a privacy perspective, the central argument in this struggle is really the following: do you, in order to operate a domain on the Internet (which is a globally accessible public resource) have to make your name, address, and phone number available to the whole world? Should that be the price of entry? Bear in mind that the WHOIS directory makes available the accredited registrar associated with every domain, so that law enforcement and civil litigants can contact the registrar to get action on any miscreants who are misusing the privilege of owning a domain.

It soon became clear, particularly in the wake of the spam explosion which took place on the Internet in 2002-2003, that individuals who put their own personal information in their WHOIS entries were having their data vacuumed up from countries they least expected, and they became vulnerable to all kinds of cybercrime. Fundamentally, the debate about being identifiable is a cost/risk assessment: should everybody be put at risk to save potential litigants and law enforcement agencies the small cost of contacting the registrar for more information?

Many of the transborder debates we are having today could be cast in this formulation: whose risks are amplified by having their data travel, and whose costs are being lowered? If, thanks to the miracle of cloud computing, my data now could be in any one of 20 global facilities for data storage, I have 20 times the risk of insider access (this is a rather simplistic example for illustration), or potentially 20 governments who might be interested in my political speech, environmental

activism, or basic freedom of expression. In addition to that, there is a risk that the service provider will be asked by a Court or the government of the country where they are incorporated, to pull the data into that jurisdiction for the purposes of giving them access.[19]

As we see the extent of profiling and intelligence gathering based on social media, routine use of the Internet that we unwittingly permit to track us (through cookies, search functions, purchase patterns etc.) and new mobile applications that track our whereabouts, we must face the fact that data protection has not been able to keep up with the pace of technological change. Are we ready for the Internet of things and the smart home, self-driving car, the tattle-tale refrigerator or heart monitor? It seems unlikely, in 2015. The question that faces all of us who want a global community where the privacy and human rights of individuals is respected, is not whether the justice system will catch up to enforce our rights; it will - as long as we do not allow those rights to be reduced. The question is, what can we do to assist?

[19] https://blogs.microsoft.com/eupolicy/2014/12/18/privacy-law-enforcement-matter-principle/