



SCALING THE VIRTUAL
TOWER OF BABEL:
LEGAL, HISTORICAL &
CULTURAL CHALLENGES
TO CROSS-BORDER
DATA FLOWS

Kenneth N. Rashbaum
Fios Consulting
New York, NY USA



Copyright © 2009, The Sedona Conference®
and Kenneth N. Rashbaum. All rights reserved.

**Scaling the Virtual Tower of Babel: Legal, Historical and Cultural Challenges to
Cross-Border Data Flows**

By

Kenneth N. Rashbaum. Esq.¹

We appear to be in the midst of a sweeping of foundations that had been in place if not for a millennium then for several centuries. . . The increased access to media affects deterritorialization because one is no longer limited to the perspectives offered by one's own home culture.”²

It is irrelevant where the electronic information is located or who, as among those entities . . . asserts ownership of the information. It is both here and there.”³

“The stakes will be rising. We need to stimulate much better compliance (with the E.U. Privacy Directives). . . Privacy is becoming a more and more relevant issue [in the] digital environment.”⁴

These are not, despite all appearances to the contrary, updated excerpts from a conversation between Alice, the White Rabbit and the Red Queen. They are, respectively, statements by a law professor, a Canadian appellate judge and European Data Protection Supervisor Peter Hustinx on the baffling intersections of traditional notions of law, privacy, culture and political boundaries in the age of digital information.

The amount of data crossing borders has increased exponentially as business increasingly globalizes. A great deal of that data is email, which is considered “personal data” in almost every country except the United States. The flow of this data crashes against the bulwarks of traditional boundaries and deep-seated jurisprudential philosophies, as well as notions of privacy informed by history and culture. Difficulties go beyond litigation; they also have consequences for enterprises attempting to, say, keep track of employees across the globe by transfer of Human Resources information, or create virtual teams world-wide to tackle the everyday problems of commercial organizations.

Conflicting notions of privacy and pretrial disclosure, and their historical and cultural underpinnings, will be discussed in this paper. It will also highlight attempts to point the way toward convergence, reaching a truce if not exactly harmony. Indeed, the inexorable march toward global globalization through electronic communications and Internet commerce makes a just resolution mandatory

¹ Kenneth N. Rashbaum is a Director of Consulting at Fios, Inc. Admitted to practice in New York and a number of federal courts, Ken has thirty years of experience as a litigator and trial lawyer, and has represented multinational clients in U.S. federal and state courts with regard to e-discovery issues and cross-border data matters. Ken is an active member of The Sedona Conference® Working Group 6 and is co-Editor-in-Chief of the White Paper . Ken speaks and writes frequently on cross-border data disclosure and business process issues.

² Berman, The Globalization of Jurisdiction, U. Conn. School of Law Articles and Working Papers. (2002) at 355 and 443, available at <http://lsr.nellco.org/uconn/ucpws/papers/13>

³ 2007 FC930 at *13

⁴ Opinion of the European Data Protection Supervisor on the Communication from the Commission to the Council on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive, available at edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.PDF

Privacy As A Fundamental Right, Privacy As a Legislated Benefit

Notions of privacy are the bedrock of the data flow dilemma. Beyond the U.S. these concepts of privacy govern disclosure of emails because email is considered “personal data;” that is, it is traceable to an identifiable individual,⁵ pursuant to E.U. Privacy Directive EC 95/46/EC and member states’ enabling legislation.⁶ Many countries outside the E.U. have either adopted this concept intact, or their privacy and data protection laws have evolved to embrace the notion that electronic communications with the name of the sender on them are entitled to privacy protection.⁷

The fundamental nature of the right to privacy outside the U.S. may be enshrined in a nation’s constitution. Article 21 of Japan’s constitution states that “the secrecy of any means of communication (shall not) be violated.” References to a right to privacy may also be found in the constitutions of Belgium. A data protection and privacy concept known as “Habeas Data” (explained more fully below) may be found in the constitutions of Brazil, Peru, Paraguay, Ecuador and Colombia.

The manner in which privacy may be regarded as closely bound to concepts of individual freedom can also be discerned by the very appellations certain countries have given to their national data protection authorities: Commission Nationale de l’Informatique et des Libertes (France); Commission de la Protection de la Vie Privée (Belgium); Guarante per la Protezione dei Dati Personali (Italy); and the Avocatul Populari (Romania) Data Protection and privacy laws directly impact the ability to transfer data between jurisdictions, and thus their historical and cultural underpinnings are the appropriate place to begin our inquiry.

Historical Antecedents

Historical experience and governmental structures inform privacy and data protection law and must be considered when discussing potential evolution of law of cross-border data flows. Privacy International has observed that “to remedy past injustices many countries, especially in Central Europe, South America and South Africa (have adopted) laws to remedy privacy violations that occurred under previous authoritarian regimes.⁸ It should come as little surprise, then, given their experiences in World War II and the Cold War, that some of the most stringent data protection and privacy laws may be found in France, Germany, Spain, Hungary, Poland and the Czech Republic. In 2008, a number of these countries’ Data Protection agencies embarked upon a program of unannounced audits and checks similar to “dawn raids” by U.S. regulatory agencies.⁹

⁵ 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 (hereafter “EC Privacy Directive”)

⁶ European Commission, *Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN (2007), available at <http://europa.eu.int>.

⁷ See *Lyondell-Citgo Refining, LP v. Petroleos de Venezuela, S.A.*, 2005 WL 1026461 (S.D.N.Y. 2005), in which the defendant, faced with a court order to produce minutes of a meeting of the Board of Directors, which would have violated Venezuela’s Special Law Against Information Systems Crimes, as the minutes evidenced the locations of named individuals (Directors) at a location and on a date certain, accepted an adverse inference instruction. Violation of The Special Law Against Systems Crimes entailed criminal sanctions.

⁸ [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559062&als\[theme\]=Data%20Protection%20and%20Privacy%20Laws](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559062&als[theme]=Data%20Protection%20and%20Privacy%20Laws), last visited May 11, 2009

⁹ What A Difference A Few Months Makes: A Changing Landscape for E.U. Data Protection Enforcement, BNA Privacy and Security Law Report, Vol. 7, No. 12, 2008 p. 439.

Historical Experience, Or Lack Thereof, Can Inform The Culture of Privacy

It is a criminal offense in France to open another's email without authorization,¹⁰ in stark contrast to the approach to employees' email in the United States. In the U.S., many corporations have protocols which state that any information placed on the corporate network is the property of the corporation and subject to monitoring and/or audit. In *Scott v. Beth Israel Medical Center*,¹¹ the court held that the plaintiff waived privilege in his communications with his attorney by transmitting those communications over the hospital's network. The court placed great emphasis on the fact that Dr. Scott had signed an acknowledgement that the network was monitored and could be accessed, and that he had acknowledged in writing that communications over that network were not private.

Many countries in South America have, perhaps in view of past experiences with authoritarian regimes, taken an approach to data protection which would appear to swing as far away from the U.S. viewpoint as possible. Data protection and privacy have evolved into a concept known as "Habeas Data." It works in practice in a way similar to its Latin root: produce the data. The emphasis is on the right of the individual to assess the data maintained about him or her. The data subject, subject to certain conditions, may request access to the data, and ask that it be corrected, amended or, in some cases, destroyed.¹² The mechanism for this scheme results in great difficulty in obtaining data for business processes, litigation or regulatory proceedings from Habeas Data countries like Brazil. As noted in the *Lyondell-Citgo* case, cited earlier, the consequences of these restrictions, for litigation, can be severe.¹³

While the source of Habeas Data is not entirely clear, one may be inclined to view Habeas Data as a natural outgrowth of the authoritarian legacy of many South American countries, since it does not bear any resemblance to European Union data protection solutions.¹⁴ Alternatively, it may be an outgrowth of culture. Japan, which has an entirely different experience with government, has a Data Protection Act which, curiously, follows a similar structure to Habeas Data. Individuals may request revision, amendment or deletion of data concerning them, and may ask that the use of their personal information cease.¹⁵ The Japanese historical antecedent for this provision may be somewhat to assess, though its roots in the cultural perspective on control of individually identifiable information may be discerned from the structure of the data protection apparatus.

States which have retained regimes which may be said to be authoritarian exercise substantial state control in their privacy and data protection laws, in some cases mitigating both privacy and protection. Russia's Constitution, in Article 23, recognizes rights to privacy and data protection, and its three data protection statutes follow roughly the format and some of the terms of the European Privacy Directives.¹⁶

¹⁰ Criminal law Article 226-15.

¹¹ 2007 N.Y. Misc. Lexis 7114 (October 17, 2007)

¹² Guadamuz A, 'Habeas Data: The Latin American Response to Data Protection,' 2000(2) *The Journal of Information, Law and Technology* (JILT). <http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html> at 9-10.

¹³ See Footnote 7.

¹⁴ *Id.* at 7.

¹⁵ Personal Information Protection Act (Law 57 of 2003), Articles 26 and 27.

¹⁶ Federal Law No. 149-FZ of July 27, 2006; Federal Law No. 152-FZ of July 27, 2006 and Federal law No. 197-FZ, dated December 30, 2001, amended as of June 30, 2006

Yet, they comprise exceptions which may be imposed by the central government for reasons of state security; there are over 30 types of classified data within forty-five laws.¹⁷

Similarly, China's Constitution provides, in Article 40, for the privacy or correspondence, but there significant exemptions for state security. While there are criminal sanctions for opening another's letter, "all international (data) connections to China go through proxy servers at official gateways, which were built with technical assistance from IBM, Cisco and Sun Microsystems. Government officials can spot individual users, monitor network traffic and filter and block content as necessary."¹⁸ It has been reported that the number of those imprisoned as a result of state surveillance has been increasing.¹⁹

As a corollary, a nation's history of experience with electronic commerce can also inform its data protection and privacy network. "As the South Korean government has a relatively long history of promoting internet use, it has a relatively long history of protecting data privacy," dating back to 1994.²⁰

Culture, history and increasing experience with global business will mold laws regarding data protection, privacy and, concomitantly, transfer of data within and from Asia over the next several years, as seen in the ongoing efforts by the Pan Asian e-Commerce Alliance (China, Japan, South Korea and Singapore) to build a commercial e-commerce network.

And these efforts will have a ripple effect far beyond Asia, since that continent, with 56.5% of the world's population also accounts for 35.8% of the world's internet use.²¹ And both figures are increasing.

National Protectionism: Blocking Statutes and Extraterritorial Jurisdiction

The combination of nationalism and protectionism, perhaps derived from an admixture of culture and history, has led some countries to raise barriers to cross-border discovery in the form of blocking statutes. These provisions prohibit the removal of commercial or technical information for use in a foreign judicial proceeding. "Blocking statutes," as described in *The Sedona Conference Framework*, "are frequently invoked in motions for protective orders with regard to discovery requests that would require cross-border transfer of electronic information. A party who discloses such information, even as part of a required investigation, may be guilty of violating blocking statutes of the country from which the data was released. Violation of a blocking statute may result in civil or criminal penalties."²²

¹⁷ See, Generally, "Russian Federation," at <http://www.privacyinternational.org/survey/phr2003/countries/russianfederation.htm>, last visited May 12, 2009

¹⁸ Kim, Y., "Data Security, Privacy In Asia," *The Seoul Times*, May 13, 2009 at <http://theseoultimes.com/ST/?url=/ST/db/read.php?id=6879>

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *The Sedona Framework® for Analysis of Cross-Border Conflicts: A Practical Guide to Navigating the Competing Currents of International e-Discovery and Data Privacy* (Public Comment Version August 2008) (hereinafter "Sedona Framework"), available at www.thesedonaconference.org, at 18

The Sedona Conference has also observed that “A number of civil law countries have also enacted blocking statutes, as a consequence of the Hague Evidence Convention, to prevent the broad reach of discovery from the United States. For example, in 1980 France specifically enacted a section of its penal law that criminalizes discovery within France by private parties for litigation abroad. French Penal Law No. 80-538 provides:

Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures.²³

In January, 2008 the Supreme Court of France indicated to the world that it takes this provision quite seriously when it published its decision affirming a criminal conviction under the statute in the matter of *In re Advocat Christopher X*.²⁴ Blocking statutes may be found in such civil law jurisdictions as Switzerland and Venezuela, and limited blocking provisions have been enacted in common law countries such as the United Kingdom, Australia and Canada.

If one may say that blocking statutes are an exercise in a form of protectionism, perhaps a more extreme form of such sentiment may be found in attempts to exert jurisdiction over information *beyond* a country’s borders, in a belief that such reach is necessary to protect the rights and benefits of its citizens. In *eBay Canada v. eBay CS Vancouver Inc. And Minister of National Revenue*²⁵, Canada’s attempt to tax certain eBay transactions was affirmed. eBay is a California corporation, and the servers where the data for the subject transactions were stored were also in California. The court ruled that the data concerning the transactions, and therefore jurisdiction to tax them, was in Canada as well as the United States because it “cannot be said to reside on only one place it is instantaneously available within the eBay entities in a variety of places . . . it is *both here and there*.”²⁶

In *Yahoo, Inc. v. La Ligue Contre Le Racisme Et L’Antisemitisme*²⁷ the United States, not to be outdone in the exercise of creative jurisdictional jurisprudence in the perceived national interest, asserted its authority over French organizations which had obtained interim orders *in France* to direct the company to cease sales of Nazi memorabilia over Yahoo! sites. The basis of the ruling was that the orders directed Yahoo to perform certain acts in California, and thus the organizations had sufficient contacts with the state of California for the district court to exercise jurisdiction.

Moving Beyond Historical and Cultural Barriers

“The frequency and intensity of (cross-border e-discovery conflicts) is heightened by an expanding global marketplace and the unabated proliferation of electronically stored information (“ESI”) . . .²⁸ Yet, there

²³ *Id.*

²⁴ Cour de Cassation, French Supreme Court, December 12, 2007 Appeal n. 07-83228

²⁵ 2007 FC 930

²⁶ *Id.* at *13 (emphasis in original)

²⁷ 433 F.3d 1199 (9th Cir. 2006)

²⁸ Sedona Framework at 1

are signs of compromise between the pull of global information flow due to expanding multinational commerce and the tug of increased concerns about technologically-driven demands on privacy.

Perhaps due to recognition of these issues, or maybe just an affinity between common-law countries, the United Kingdom and the United States have exhibited signs of convergence in data disclosure/discovery. In the case of *Digicel v. Cable & Wireless PLC*²⁹ the High Court for England and Wales was presented with the question (among other issues) of whether the parties should have reached agreement on search terms before the defendant searched utilizing only its own terms. U.K. procedures around pre-trial disclosure, while more liberal than those in the rest of Europe, have traditionally diverged from the more expansive discovery in the U.S. Yet the court in *Digicel*, in ordering the defendant to search again, cited as authority for its holding a U.S. case, *Zubulake v. UBS Warburg*³⁰, and *The Sedona Principles*. These authorities were cited for, ironically, the *scope of disclosure* in U.K. dispute.³¹

Yet, *Digicel* was not the first instance of a British court hewing close to U.S. perspective. The U.S. takes a more restrictive view of the concept of personal data than the E.U., considering that term to refer to data which describes or otherwise refers to aspects of an individual. In 2003 the Supreme Court of Judicature Court of Appeal (Civil Division) considered the issue of how “personal data” should be construed in *Durant v. Financial Services Authority*.³² The claimant had previously commenced litigation against Barclays Bank PLC, which he lost in 1993. Durant sought certain data which named him to assist him in reopening his claim, and asserted that the data held by defendant FSA, a data controller for Barclays, in that U.K. legislation gave individuals a right to access of their “personal data.” FSA declined on the ground that the information sought was not “personal” within the meaning of the 1998 Data Protection Act, which was the enabling legislation for E.U. Privacy Directive 95/46 EC. The court disagreed, holding that “in conformity with the (the statutes) and the Directive. . . it is likely that in most cases only information that names or directly refers to him will qualify.”³³

The Asia-Pacific region has ascertained a need to find some resolution of e-discovery and cross-border data flow disputes. The Asia-Pacific Economic Cooperation Steering Group has moved forward on its 2004 Privacy Framework, with the intention to “facilitate responsible information flows, which creates an essential basis for increased trade and e-commerce to flourish.”³⁴ On February 11, 2009 Australia finalized Practice Note 17, which requires that the parties come to a conference similar to the “Meet-and-Confer” in the U.S. and U.K., prepared with a checklist for e-discovery items. The Note also includes an exemplar “Advanced Document Management Protocol.”³⁵

And the European Commission’s Article 29 Working Party, while noting the continuing “tension between the disclosure obligations under U.S. litigation or regulatory rules and the application of the data protection requirements of the E.U., acknowledged in its Article 29 Working Party Working Document 1/2009 that it “sees the need for reconciling the requirements of the U.S. litigation rules and the E.U. data

²⁹ [2008] EWHC 2522 (Ch)

³⁰ 217 F.R.D. 309 (S.D.N.Y. 2003).

³¹ *13, 2008 EWHC 2552 (CH)

³² [2003] EWCA Civ 1746

³³ *Id.* at *9.

³⁴ APEC Fact Sheet, http://www.apec.org/apec/news_media/fact_sheets/apec_privacy_framework.html, last visited May 13, 2009

³⁵ Federal Court of Australia, Practice Note 17, available at http://www.fedcourt.gov.au/how/practice_notes_cj17.htm

protection provisions.”³⁶ Recognition of the requirements of global commerce and respect for privacy are slowly moving closer together, scaling the walls of history, culture and jurisprudential distinctions.

Courts, litigants and business stakeholders, whose expenditures for counsel and consultants to bridge these gaps consistently trend upward, are anxiously watching their progress.

³⁶ Article 29 Data Protection Working Party *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, adopted on 11 February 2009, available at http://ec.europa.eu/justice_home/fs/privacy/index_en.htm, at 2.