University of Miami International and Comparative Law Review

Volume 18
Issue 2 *Volume 18 Issue 2 (Spring 2011)*

Article 3

4-1-2011

¿Viva La Data Protection? Chile As A Touchstone For The Future Of Information Privacy

Nicola Carah Menaldo

¿*VIVA LA* DATA PROTECTION? CHILE AS A TOUCHSTONE FOR THE FUTURE OF INFORMATION PRIVACY

Nicola Carah Menaldo

FOREWORD: This article attempts to uncover a puzzle: although the traditional levers for strong privacy protection are present in Chile – a history of dictatorship, an information technology revolution, and strong trade with the European Union – its data protection laws are in fact very weak. What explains this apparent disconnect? This article challenges the conventional wisdom that Chile's weak data protection regime is the result of weak democratic institutions, collective action problems, or the prioritization of credit data protections. Instead, it argues that Chile's stunted regime results from a political culture in which privacy protections, generally, are traded off for other, competing values, including free speech and the free-flow of information. These conclusions suggest that proponents of present and future efforts to harmonize data protection law on a global basis may need to more fully address divergent cultural conceptions of privacy world-wide. Such proponents might also more fully consider the loss of cultural pluralism that will necessarily ensue from any successful global data protection harmonization scheme.

I. INTRODUCTION

Chile's brand of information-privacy affords limited individual rights for data subjects and undercuts implementation and enforcement – an information status quo that differs significantly from that in the United States and Europe. For instance, voter rolls are publicly disclosed by the government and sold for direct marketing purposes.[1] There is a national ID system, wherein every citizen is provided with an identification card at birth bearing a number that later becomes his or her driver's license and passport number. Business owners routinely require the provision of this ID number in addition to a signature on every credit card transaction. As a hacker named "Anonymous Coward" pointed out when he leaked the personal information of over six million Chileans on the Internet in May of 2008, the military, regulatory, and private sectors

---

[1] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 30 (1999).

all collect and store massive quantities of personally identifiable information on a regular basis.[2] What legal and administrative foundation supports such a patent infringement of the individual right to privacy?

While debate has raged on in the United States and Europe about how to approach data protection in an increasingly digitized world, and how this fits into larger conceptions of privacy, very little attention has been paid to the world's newest constitutional republics that most resemble our own: the countries of Latin America. What of their privacy and data protection laws? If there are gaps or deficiencies in privacy and data protection legislation in Latin America, what can anybody else do about it?

This paper attempts to answer these questions by taking a close look at Chile and how that country has approached the question

---

[2] In the early hours of May 10, 2008, a hacker called "Anonymous Coward" posted the personal information of over 6 million Chilean citizens on the Chilean technology blog, FayerWayer. The posted data included names, personal identification numbers, street addresses, telephone numbers, and educational records of over half of the country's population. In a readme.txt file left with the data, the hacker reported that the information had been pilfered from the Ministry of Education, the Directorate of National Mobilization (a military branch), the Electoral Service, and several telephone databases. The hacker also pointed out that, using Google maps and Google earth, the data he supplied could be used to create a virtual map of where each of the affected residents live. Further, by aggregating the school data and subway pass data that was also posted, one could show the comings and going of any individual person in the dataset. The hacker's motive, the file said, was to "show how poor data protection is in Chile." D. Muñoz, P. Orellan & Ó. Saavedra, *Cibercrimen investiga filtración de bases de datos personales de seis millones de chilenos,* EL MERCURIO (May 11, 2008), http://diario.elmercurio.cl/detalle/index.asp?id={0f85cc8b-2085-468b-bc5d-1aea14ab5a18 (author's translation). *See also* JI Stark, *ALERTA: Se filtran datos personales de 6 millones de chilenos vía Internet,* FAYERWAYER (May 10, 2008), http://www.fayerwayer.com/2008/05/alerta-se-filtran-datos-personales-de-6-millones-de-chilenos-via-internet; *see also Hacker leaks 6m Chileans' records,* BBC NEWS, http://news.bbc.co.uk/2/hi/americas/7395295.stm; *Hacker gets into Chilean government files, leaks personal data to Internet,* THE ECONOMIC TIMES (May 11, 2008), http://www.iht.com/articles/ap/2008/05/11/america/LA-GEN-Chile-Data-Leaked.php; Traian Teglet, *Personal Data of Six Million Chileans Available on the Internet,* SOFTPEDIA (May 12, 2008), http://news.softpedia.com/news/Personal-Data-of-Six-Million-Chileans-Available-on-the-Internet-85353.shtml.

of data protection and information privacy at the legal level.[3] It will uncover a puzzle: although the traditional levers for strong privacy protection are present in Chile – a history of dictatorship, an information technology revolution, and strong trade with the European Union[4] – its data protection laws are in fact very weak. What explains this apparent disconnect?

This article will show that this is likely the result of a cultural attitude towards privacy that varies widely from that in industryalized countries. Legal theorists have long maintained that there is an inextricable link between national culture and legal regimes.[5] More recently, researchers have shown through empirical studies that such a connection exists. In a study on comparative regulatory approaches to corporate information management systems, Milberg, Smith, and Burke identified varying cultural conceptions about privacy across countries.[6] They then compared those conceptions to the data protection regulations in place in those countries.[7] They found that a given country's regulatory approach to corporate information management was affected by culture.[8] "[D]ifferences in

---

[3] While there is undoubtedly a technological aspect to privacy and data protection, especially upon determining the cause of a single data leak, this paper will focus primarily on the legal structure behind privacy and data protection in Chile. *See* Banisar & Davies, *supra* note 1, at 14 (noting that a European Council evaluation of several technologies of privacy could likely supplement but not replace legal protections).

[4] *See* Banisar & Davies, *supra* note 1, at 14; Warren B. Chik, *The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore – Two Differing Asia Approaches*, 14 INT'L J.L. & INFO. TECH. 47 (2006); *See also* Miriam Wugmeister, Karin Retzer, & Cynthia Rich, *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 GEO. J. INT'L L. 449 (2007).

[5] *See, e.g.*, LAWRENCE ROSEN, LAW AS CULTURE: AN INVITATION xii (2006) ("[L]aw is so deeply embedded in the particularities of each culture that carving it out as a separate domain and only later making note of its cultural connections distorts the nature of both law and culture.").

[6] Sandra J. Milberg, H. Jeff Smith, & Sandra J. Burke. *Information Privacy: Corporate Management and National Regulation,* 11 ORGANIZATION SCIENCE 35 (2000).

[7] *See id.*

[8] *Id.*

political systems and legislation in various countries," they wrote, "can be interpreted as consequences of societal value differences."[9]

One of the study's central findings was that countries with high levels of "individualism" exhibited higher levels of concern for information privacy.[10] This finding accords with Dutch researcher Geert Hofsteed's findings, which showed high levels of individualism in European countries compared to countries around the world.[11] Latin American countries exhibited low levels of individualism.[12] This contrast in cultural individualism between Europe and Latin America correlates with the contrast in legal protections of information between these two regions.[13]

Culture is a compelling predictor of whether or not a particular country will adopt stringent legal privacy protections for information. This is because cultural conceptions of privacy can vary significantly between countries. In other words, there is no singular normative value that dictates the optimum level of privacy across all individuals in all contexts. In addition, researchers have long noted a significant link between cultural norms and legal norms within a

---

[9] *Id.* at 40.

[10] *Id.*

[11] Where individualism was scored on a sliding scale from 0 to 100, and where 100 represented high levels of individualism and 0 represented low levels, European countries scored an average score of 65 and a median score of 70.5. This is well above the mean score of 43.1 for all countries sampled. *See generally,* GEERT HOFSTEDE, CULTURES AND ORGANIZATIONS: SOFTWARE OF THE MIND 53 (1991).

[12] The Latin America average is 21, and the median is 16. This is well below the mean score of 43.1 for all countries sampled. *Id.*

[13] Hofsteed's individualism scores may even help explain the variation *within* Latin America: of the thirteen Latin American countries studied in Hofsteed's sample, Argentina scores the highest on the metric of individualism, with a score of 46. This was well above the regional average of 21. In fact, Argentina's individualism score is higher than those of both Greece (35) and Portugal (27). Not surprisingly, Argentina has the most robust privacy regime in Latin America. Chile, on the other hand, scores a 23 in individualism. This is close to the regional mean of 21, and far below the European mean of 65. While the relationship between the individualism exhibited in a country's culture and the relative strength to which they give their data protection laws is robust, it of course is not a perfect correlation. The outlier is the United States, which has the highest individualism score of the sample (91), yet has weaker information privacy protections than much of Europe (as indicated by the EU's reluctance to deem the US as having "adequate" safeguards under the EU Directive). *Id.*

nation. One would imagine then that varying conceptions of privacy would lead to variations in legal approaches to data protection, depending on the degree of cultural concern surrounding privacy in any given country. Finally, emerging research has begun to show such a correlation: those cultures that value privacy highly tend to adopt strict data protection regimes and those that do not tend not to follow suit. In other words, culture explains variation in data protection regimes across countries, because (a) cultures vary from one country to another, (b) there is a growing consensus that culture affects legal schemes adopted by lawmakers, and (c) there is mounting research that variation in privacy regimes track variations in national culture.

Part II of this paper will show that, despite many indicators that predict that Chile would have relatively strong privacy and data protection laws, its legislation in this realm is actually very sparse in comparison to the U.S. and Europe. It will also provide a brief overview of the modern history of privacy legislation in the U.S. and Europe, where privacy concerns have been strongest, and explain some of the theories for the modern surge in privacy legislation. Part III will suggest that the reason that Chile has not joined this trend can be attributed to the fact that cultural norms about privacy differ significantly between countries and that the Chilean political culture is one where privacy protections have been traded off for other, competing values. Finally, Part IV will argue that present and future efforts to harmonize privacy law on a global basis will be unsuccessful unless recognition is given to divergent cultural conceptions of privacy, suggesting that one cannot achieve legal harmonization without some degree of cultural homogeneity.

II. CHILE'S SURPRISINGLY WEAK INFORMATION PRIVACY REGIME

A. Mapping Out Chile's Weak Information Privacy Regime

Paradoxically, Chile's legal system *appears* to vigorously protect the privacy of personal information. Indeed, the right to privacy is explicitly enshrined in Chile's 1980 Constitution, in sharp contrast to the constitution of the United States and some Common-

wealth countries.[14] Article 19 of the Chilean Constitution guarantees, "[r]espect and protection for public and private life, the honor of a person and his family" as well as, "[t]he inviolability of the home and of all forms of private communication."[15]

In addition to this constitutional guarantee, Chile has also passed specific legislation relating to information privacy and data protection. Chile's first piece of data protection legislation, called the "Law for the Protection of Private Life" (the "Privacy Act"),[16] was passed on October 28, 1999. It was the first such information privacy law to be enacted in Latin America.[17] The Privacy Act was modeled after Spain's Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data (subsequently amended by Organic Law 15/1999 on the Protection of Personal Data)[18], and sought to provide a comprehensive regime for the treatment of personal information of all types, in both the private and public sectors.[19] The Privacy Act remains central to Chile's data protection regime to this date, notwithstanding minor changes to the law enacted in 2002.[20] As a result,

---

[14] *Id.* Although these documents have been interpreted to contain similar protections, they not explicitly protect the individual's right to privacy.

[15] CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE [C.P.] art. 19.

[16] Law No. 19628, Octubre 28, 1999, DIARIO OFICIAL [D.O.].

[17] Luis Salazar, *Beyond EU: Privacy and Security Law Developments of Interest to U.S. Companies Doing Business in Latin America,* 934 PLI/PAT 733, 743 (2008).

[18] *Protección de datos: mucho más que privacidad personal,* BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE (Nov. 3, 2006), http://www.bcn.cl/noticias/proteccion-de-datos-mucho-mas-que-privacidad-personal; Pedro Anguita R., *Jurisprudencia Constitucional Sobre el Derecho a la Propia Imagen y a la Vida Privada en Chile (1981-2004): Un Intento de Sistematización, in* LIBERTAD DE EXPRESIÓN EN CHILE 319, 488 n. 127 (Facultad de Derecho de la Universidad Diego Portales ed., 2006).

[19] Salazar, *supra* note 17. As will be discussed in Part II, *infra,* this model most closely resembles the European Union's approach to data protection legislation as embodied, for example, in the EU's Directive on the "protection of individuals with regard to the processing of personal data and on the free movement of such data." In contrast, the United States has chosen to approach the information privacy legislation through a series of sector-specific laws, such as the Video Privacy Protection Act and the Fair Credit Reporting Act.

[20] Law No. 19628, Agosto 28, 1999, DIARIO OFICIAL [D.O.], *available at* http://www.bcn.cl/leyes/pdf/actualizado/141599.pdf; Law No. 19628, Junio 28, 2002, DIARIO OFICIAL [D.O.], *available at* http://www.gennoa.com.ar/system/files/ 19812-ModifProteccion+datos+personales.pdf.

much of the discussion regarding Chile's data protection regime will center on the concepts and implications of the 1999 Privacy Act.

The core principles of Chile's Privacy Act are trifold. First, the law provides for informed consent and legality: information can only be collected from individuals who give consent, when told of the purpose of its collection, and if authorized by law.[21] Second, the Privacy Act addresses access, rectification and removal: individuals can demand access to information collected about them, and can require correction or removal of such information.[22] The third principle is "purpose": with the exception of journalistic information, information can only be used for the purpose for which it was collected.[23]

The specific provisions of the Privacy Act flesh out these core principles in more detail. For example, in the public sector, an entity can only collect data relating to the areas of its competency.[24] The Civic Registration and Identification Service is charged with maintaining a central, public database of every database held by a public entity within the country. Upon registration of an individual database, the public entity that owns the database must provide information concerning the legal basis for its maintenance, its purpose, the type of data stored, and the universe of people it includes.[25]

When an individual in Chile demands that a public entity provide her with access to her personal information, the database holder is required to respond within two working days.[26] If the database holder fails to respond within this time frame, the owner of the information can demand the information before a local judge. The law establishes a summary proceeding and special procedural

---

[21] Banisar & Davies, *supra* note 1.

[22] *Id.*

[23] *Id.*

[24] SEBASTIÁN RÍOS LABBÉ, LA PROTECCIÓN CIVIL DEL DERECHO A LA INTIMIDAD 133 (2003).

[25] *Id.* at 135.

[26] *Id.* at 137. While many commentators have noted that Chile's privacy legislation more closely mirrors European legislation, at least on its face, than it does neighboring Latin American countries', this provision actually resembles the habeas data approach taken by Brazil and others. Thus, the more accurate description of the form of Chile's legislation is likely somewhere in between European-style laws and those of Latin America.

rules to expedite cases involving the request of personal information.[27] Defenses for failing to provide the information are limited to showings that the provision of the information will impede the functions of taxing by a duly appointed public organ, affect the secrecy established in legal or regulatory dispositions, or implicate national security or the national interest.[28]

If the reason for not providing the information is national interest or national security, the forum for complaint changes to the Supreme Court.[29] The minimum penalty is 1 Monthly Taxation Unit (UTM) and the maximum penalty is 50 UTMs.[30] In addition, if the failure to provide information is unwarranted, courts have the discretion to suspend the head of the offending public organ for five to fifteen days.

Title III of the Privacy Act is dedicated to the treatment of personal financial information and it establishes the type of economic and financial information that may be known and kept by a database older.[31] This section also stipulates that financial information regarding debts cannot be kept for more than ten years, or three years after discharge.[32] The latter limit was lowered to seven years with the passage of the 2002 amendment.[33]

Chile's combination of constitutional and legislative protections of information privacy certainly looks great on paper. However, there are three overlapping reasons why Chile's data protection is relatively weak in practice. First, there are constitutional reasons: constitutional history precludes persuasive use of any constitutional

---

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.* at 138. The UTM is a monetary unit that is adjusted monthly for inflation and that is used by the Chilean government in collecting taxes and sometimes, as here, in setting fines. The value of 1 UTM in March, 2009 was Cl$ 36,866.00 or US$ 63.14. *See* BANCO CENTRAL DE CHILE, MONTHLY TAX UNIT (UTM) INTERNAL REVENUE SERVICE (2009), *available at* http://www.bcentral.cl/eng/economic-statistics/series-indicators/index_ps.htm.Thus, the maximum penalty for violating the Chile's Privacy Act is US$ 3,157.00.

[31] The 2002 amendments removed public utility debt from this list of collectible information. LABBÉ, *supra* note 24.

[32] *Id.*

[33] *Id.*

privacy protections in the data protection context. Second, there are structural problems with the law: the Privacy Act fails to secure many necessary rights to prevent the dissemination of private information, and, even where those rights are secured, fails to provide for the institutional mechanisms necessary to enforce those rights. Third, there are significant compliance problems: even where the rights and institutions are nominally in place, there is widespread lack of compliance and enforcement of legal information privacy laws.

1. Constitutional Deficiencies

To begin with, Chile's Constitutional protection of private life was written before many of today's threats to information privacy had even been conceived. In 1980, when the constitution was enacted, the Internet was still being built by a handful of university and government researchers[34] and computer-processing speeds were many times slower than they are today. Thus, privacy protections enshrined in Chile's constitutional document embodied conceptions of privacy that likely had little to do with data protection and information privacy.[35] It is likely, for instance, that sub-article 4 of article 19, providing "respect for and protection of private and public life and the honor of the individual and his family," was at least partly about enshrining Chile's version of libel (*injurias*) in the Constitution.[36] Indeed, until recently, the sub-article read, in its entirety:

> Respect for and protection of private and public life and the honor of the individual and his family. Violation of this precept, committed through a mass medium, whereby a false deed or action is imputed

---

[34] JOHNATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 26-28 (Yale University Press 2008).

[35] *See* PEDRO ANGUITA R., LA PROTECCIÓN DE DATOS PERSONALES Y EL DERECHO A LA VIDA PRIVADA 223 (2007).

[36] The *injurias* offense, unlike defamation, can be shown not only by proving harm to public esteem, but also through a subjective standard, whereby injuries to self-respect or family honor also constitute elements of the crime. Unless the victim is a public figure and the offense relates to that person's public office, the truth of the disputed statement is no defense. *See* SEBASTIAN BRETT, LIMITS OF TOLERANCE: FREEDOM OF EXPRESSION AND THE PUBLIC DEBATE IN CHILE 46 (1998).

> unjustifiably causing harm or discredit to an individual or his family, shall constitute a crime and shall be punished as determined by law. However, the mass medium may claim exception by proving, before the corresponding court, the truth of the imputation, unless it should constitute in itself a libel against private individuals. Furthermore, the proprietors, editors, directors and administrators of the respective mass medium shall be jointly responsible for the appropriate indemnifications.[37]

Thus, the language that followed the constitutional right to private life was viewed by many as limiting the provision to very specific applications in the defamation and libel contexts. It was only in 2005, after tremendous pressure from human rights organizations and the press, that the Chilean congress passed a constitutional amendment to remove all but the first sentence from this sub-article.[38] It is not until recently that it would have made sense to interpret this provision in the more ample sense of requiring it to be applied in the realm of personal data protection. Accordingly, courts have been reluctant to extend constitutional protections of privacy to the realm of personal data protection and information privacy.[39]

2. Legislative Deficiencies

Even if the constitution does not provide for strong data protection on its own, it may appear on its face that Chile's Privacy Act successfully fills the gap. The Privacy Act, however, does far less to prevent the widespread dissemination of personal information than would be expected from a law that appears to have been adopted for such a purpose. The law fails both to secure the

---

[37] CONSTITUCIÓN POLITICIA DE LA REPUBLICA DE CHILE [Constitution] (1980), absent amendments, *available at* http://confinder.richmond.edu/admin/docs/ Chile.pdf.

[38] Reforma Constitucional que Introduce Diversas Modificaciones a la Constitución Politica de la Republica de Chile [Constitutional Reform that Introduces Several Modifications to the Political Constitution of the Republic of Chile], Law 20050, art. 1, 10(b), Agosto 26, 2005, DIARIO OFICIAL [D.O.].

[39] ANGUITA, *supra* note 35.

necessary rights to protect personal information, and to define institutional mechanisms necessary to enforce those rights.

One of the central deficiencies of the Chilean data protection legislation as it stands today is that, in many instances, it fails to require consent before information is collected or disseminated. For instance, public entities do not need to obtain the consent of the data subject when it collects information related to the areas of its competency.[40] In addition, and in contrast to most comprehensive data protection regimes in Europe, Chilean law does not require that data subjects be informed in an express, precise and unequivocal manner before data is collected from them. Instead, the Privacy Act uses the more vague "express consent" standard. [41] Finally, the Chilean data protection law explicitly eliminates such an express consent requirement in instances where the treatment of personal data was derived from public sources and is "necessary for direct response commercial communications, or the direct commercialization or sale of goods or services."[42]

Individual rights are watered down in Chile's data protection regime in other ways as well. For instance, all of the rights provided for by the Privacy Act are qualified by exceptions - namely, one cannot request information, modify, cancel or block personal data when doing so would interfere with taxing functions or the secrecy established in regulatory and legal proceedings, or where it would affect that national interest.[43] While these exceptions are significant, perhaps the largest exception is for information that would "affect . . .

---

[40] Law No. 19628, art. 20, Agosto 28, 1999, DIARIO OFICIAL [D.O.]; *see also* LABBÉ, *supra* note 24.

[41] Instead, Article 4 provides that "The treatment of personal data can only occur when authorized by this law or other legal disposition or the data subject expressly consents to it. The person that authorizes it should be duly informed about the purpose of the storage of its information and its possible communication to the public. The authorization should be in writing." Law No. 19628, art. 4, Agosto 28, 1999, DIARIO OFICIAL [D.O.] (author's translation); *see also* ANGUITA, *supra* note 35, at 306.

[42] Law No. 19628, art. 20, Agosto 28, 1999, DIARIO OFICIAL [D.O.] (author's translation).

[43] *Id.* art. 15.

national interest," where "national interest" is left otherwise undefined in the statute.[44]

Chile's Privacy Act is also the only data protection law in the world that explicitly protects the individual right to handle personal data. [45] Because processing personal data is not prohibited and does not constitute otherwise illicit behavior, commentator Pedro Anguita posits that codifying such a right is absolutely unnecessary.[46] While it is not clear that codifying such a right to process information substantively affects courts' interpretation of the Privacy Act, it is likely that such codification inherently weakens privacy protections by creating a conflicting statutory right that must be balanced against the right to privacy.[47]

3. Institutional Deficiencies

Beyond ample qualifications to the rights enunciated in Chile's Privacy Act, there are a number of structural components that serve to further weaken Chile's privacy regime. First, while the law mandates that a central, public database be created of all databases maintained by public entities in the country, no separate privacy commissioner or agency has been created to administer it. Instead, the law places this responsibility on the "Service of Civic Registration and Identification," (the "Service") an already overburdened institution with information processing needs and problems of its own.[48]

Indeed, the Service was hamstrung in performing its duties under the Privacy Act from the outset. The Privacy Act was passed without any corresponding budget, so the Service was not and has never been allocated any additional funds for instituting or maintaining the central database in its charge.[49] In addition, the

---

[44] *Id.*

[45] ANGUITA, *supra* note 35, at 305; Law No. 19628, art. 1, Agosto 28, 1999, DIARIO OFICIAL [D.O.] ("Every person may handle personal data as long as they do so in a manner that is compliant with the law and is for purposes permitted by judicial order. In any case one should respect the exercised of the fundamental rights of the owners of the data and the ability that this law gives them.") (author's translation).

[46] ANGUITA, *supra* note 35, at 305.

[47] *See id.*

[48] LABBÉ, *supra* note 24, at 135.

[49] ANGUITA, *supra* note 35, at 328.

Service has no authority to enforce any of the rights enumerated in the statute. It cannot require that any public entity register its database with the Service and it has no authority to assist citizens in obtaining access, modifying, canceling or blocking access to their personal information where that information has not been registered. This, some contend, is one of the worst and most notorious defects of the Chilean data protection system.[50] Even if all public entities were to register their databases with the Service - which they do not[51] - because there is no corresponding requirement for private database holders, individuals would remain largely unaware of the information that has been collected about them in the private sector.[52]

In addition to the structural problems that stymie any attempts to carry out registration requirements, the law also fails to provide adequate incentives for compliance with the law. Critics contend, and the evidence suggests, that the fine for failing to comply with the Privacy Act (the maximum fine is approximately $ 3,000) is too small to create any meaningful disincentive.[53] Furthermore, there is no provision for the payment of attorneys' fees, damages, or other incentives to encourage "private attorney generals" to bring suits on behalf of individuals on a contingency fee basis. Instead, if an individual has a claim under the Privacy Act, she must pay for an attorney to do so on her behalf. If she wins the suit, she gains access (or modification, cancellation or blocked access to) her information and nothing else. Finally, since individuals can only bring claims on behalf of themselves, there is no possibility for class action type litigation or even claims on behalf of one's self and one's family members. Because of these constraints, some critics contend that

---

[50] *Id.*

[51] Interview with Juan Pablo Olmedo, President of Transparency Council, in Santiago, Chile (Jan. 12, 2009).

[52] *See* ANGUITA, *supra* note 35, at 328 (contrasting some of the more restrictive regimes, e.g., Sweden, that require registration of any and all public and private databases in the state).

[53] *Id.* at 338.

what the law really protects is the economic order, not the privacy of individuals.[54]

B. Grounding the Issue: the Modern History of Privacy Legislation

When compared against the yardstick of the evolution of modern information privacy law, it is clear that Chile's Privacy Act cannot be counted among the most robust data protection schemes in the world. Before explicating the role played by Chile's political culture in explaining its surprisingly weak data protection regime, it is valuable to review the historical background of information privacy protections.

1. Early Privacy Initiatives

International recognition of privacy as a human right began after World War II, when several international human rights instruments incorporated a right to privacy in their texts.[55] The first international document to address the right to privacy was the International Declaration of Human Rights, which was adopted by the UN General Assembly on December 10, 1948, but was not binding on member countries.[56] In articulating the right to privacy, the UN General Assembly resolution focused specifically on the inviolability of the home and the right to secrecy in communications.[57] The text reads:

> No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor or reputation. Everyone has

---

[54] *Proteccion de datos: mucho mas que privacidad personal*, BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE (Nov. 3, 2006), http:www.bcn.cl/noticias/proteccion-de-datos-mucho-mas-que-privacidad-personal.

[55] *See* THE GLOBAL ENCYCLOPEDIA OF DATA PROTECTION REGULATION 1 (Jan Holvast, Wayne Madsen, & Paul Roth eds., 1999) [hereinafter GLOBAL ENCYCLOPEDIA].

[56] *Id.*; *see also* Universal Declaration of Human Rights, G.A. Res. 217A, at 71, U.N GAOR, 3d Sess., 1st plen. mtg., U.N. Doc A/810 (Dec. 12, 1948).

[57] Banisar & Davies, *supra* note 1, at 8.

> the right to the protection of the law against such interferences or attacks.[58]

The right to privacy as articulated in the Universal Declaration of Human Rights was incorporated in a number of international instruments that followed. These subsequent instruments were binding on those countries that ratified them, and included: the 1948 American Declaration of the Rights and Duties of Man, 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, 1966 International Covenant on Civil and Political Rights, and 1969 American Convention on Human Rights.[59] In addition, the right to privacy, as articulated in the Universal Declaration on Human Rights, was also incorporated in the UN Convention on Migrant Workers and the UN Convention on the Rights of the Child.[60] In many of these instruments, the right to privacy also serves as an underpinning of other important rights and values, such as the rights to freedom of association and freedom of speech and the value of human dignity.[61]

Many countries that enacted constitutions after the proliferation of International Human Rights instruments after World War II incorporated the right to privacy, as articulated in these instruments, into their national constitutions. However, even many of those countries with constitutions that pre-date the International Human Rights era also have some version of the right to privacy enshrined in their founding documents. [62] In many countries that do not explicitly recognize a right to privacy in their constitution, courts have nonetheless interpreted other provisions as incorporating that right.[63]

---

[58] Universal Declaration of Human Rights, G.A. Res. 217A at 71, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948).

[59] GLOBAL ENCYCLOPEDIA, *supra* note 55, at 1-2; *see also* Banisar & Davies, *supra* note 1, at 3.

[60] Banisar & Davies, *supra* note 1, at 9.

[61] *Id.* at 3.

[62] *Id.*

[63] The implied right to privacy in the United States Constitution as interpreted by the United States Supreme Court is a paradigmatic example of such an approach. Ireland and India are two other countries that have taken this route. *See Id.*

The result is that the vast majority of countries include some version of the right to privacy in their constitution.[64]

A second wave of concern for the right to privacy occurred in the late 1960s and it was at this time that the concept of data protection as a piece of the debate came into being. European countries were the first to take steps to proactively protect data.[65] The state of Hesse in Germany was the first to adopt a data protection law in 1970.[66] In 1973, Sweden became the first country to adopt a national data protection law.[67]

2. The Consolidation of Data Protection Regimes

As individual European countries began to approach the issue of data protection, more comprehensive European regimes sprouted up as an effort to harmonize these laws. Thus, in 1981, the Council of Europe passed the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.[68] Shortly thereafter, the Organization for Economic Cooperation and Development instituted Guidelines for the Protection of Privacy and Transborder Data Flows of Personal Data (the "OECD Guidelines").[69] The stated purpose of the OECD Guidelines was not to protect privacy, per se, but to encourage countries to cease passing data protection laws that effectively caused impediments to the flow of data across borders. The guidelines, which were voluntary, were expressed in very broad terms in order to afford individual countries the flexibility to enact their own legislation.[70]

The 1995 European Parliament and Council directive on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data" (the "EU Directive") is

---

[64] *Id.*

[65] GLOBAL ENCYCLOPEDIA, *supra* note 55, at 2.

[66] *Id.*

[67] *Id.*

[68] Banisar & Davies, *supra* note 1, at 10-11.

[69] *Id.* at 11.

[70] *See* Ryan Moshell, *...And then There was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection,* 37 TEX. TECH. L. REV. 357, 365 (2005).

the Gold Standard of data privacy protection.[71] Unlike the OECD Guidelines, the EU Directive was motivated less by economic concerns about impeding the free flow of information and more by human rights concerns surrounding individual rights and the right to privacy. [72] The Directive was written as a mandatory law and required member countries to pass laws that incorporated the Directive principles by 1998. One of the central requirements of the EU Directive is that EU countries ensure that personal data flowing from their country to any non-EU state is adequately protected by the foreign state. As a result of this provision, six countries have been accredited as providing "adequate" privacy protection. The United States has negotiated a separate safe harbor agreement.

The EU Directive has had a profound effect on the shaping of European information privacy regimes. For example, researchers have found that, because of the Directive, European data protection laws tend to converge on seven core principles. Namely, all information must be:

1. Obtained fairly and lawfully
2. Used only for the original specified purpose
3. Adequate, relevant and not excessive to purpose
4. Accurate and up to date
5. Accessible to the subject
6. Kept secure
7. Destroyed after purpose is completed[73]

In addition, all EU countries are required to appoint a Commissioner, Ombudsman or agency responsible for protecting information rights.[74] Many countries have taken the additional (voluntary) step of requiring that public and some private databases be registered, or

---

[71] Banisar & Davies, *supra* note 1, at 4.

[72] GLOBAL ENCYCLOPEDIA, *supra* note 55, at 2.

[73] Banisar & Davies, *supra* note 1, at 11; *see also* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace,* 52 STAN. L. REV. 1315, 1328 ("Surprisingly, in all of the major international efforts that have so far addressed . . . [data protection], there has been a broad measure of agreement on the 'basic rules' around which domestic privacy legislation should cluster.").

[74] Banisar & Davies, *supra* note 1, at 12.

even that the appointed privacy agency pre-approve any proposed processing of personal data.[75]

3. Data Protection Beyond Europe

Outside of Europe there has also been a resurgence of concern privacy in the form of data protection legislation, but approaches to the problem have been more diverse. Whereas Europe took the approach of comprehensive data protection, built on a rights-based conception of data protection as an outgrowth of the right to privacy, and thus encompassing all realms data collection and processing, other nations have adopted other methods of regulation in many cases.[76] Banisar has identified three types of modern data protection regimes: the "Comprehensive Model," the "Sectoral Legislation Model" and the "Self-Regulatory Model."[77] Other scholars also use this taxonomy with slight variations.[78] There is also a fourth approach that only exists in Latin America called the "habeas data" model.

The Comprehensive Model for data protection is most prevalent in Europe, although Canada and Australia have also taken this approach.[79] In countries that employ this type of regime, there is usually a privacy commissioner, ombudsman or agency that is appointed with the task of enforcing and/or administering the information privacy law. Sometimes this entity will be given the power to find against an offender, but its responsibilities can vary. Data protection laws under this approach generally apply to both the private and the public sectors.[80] Nonetheless, in some countries, the legislative body creates the general framework and appoints a statutory body to regulate and enforce the law, but also leaves a

---

[75] Tim Wu, *The International Privacy Regime, in* SECURING PRIVACY IN THE INTERNET AGE 92, 98 (Anupam Chander, Lauren Gelman, & Margaret Jane Radin eds. 2008).

[76] *See* Chik, *supra* note 4, at 76-77; Banisar & Daives, *supra* note 1, at 14; Reidenberg, *supra* note 73, at 1330-31.

[77] Banisar & Davies, *supra* note 1, at 13-14.

[78] *See, e.g.*, Chik, *supra* note 4, at 56-66; Reidenberg, *supra* note 73, at 1330-1332.

[79] Banisar & Davies, *supra* note 1, at 13-14.

[80] Chik, *supra* note 4, at 76.

certain amount of room for individual industries to create and enforce their own rules.[81]

A Comprehensive Model approach to data protection law likely offers the highest level of protection to individual information privacy. For many scholars, the Comprehensive Model represents the pinnacle of data protection and serves as the yardstick against which all other data protection regimes are measured.[82] Critics, however, contend that such an approach is too harsh and too costly, especially in those cases where the scope of protection seems excessive.[83]

The "Sectoral Legislation Model" is the model of data protection that is used in the United States. In addition, some countries complement a comprehensive approach with specific sectoral laws.[84] Under this model, there is no central comprehensive legislation that governs the protection of all kinds of data. Instead, laws are passed on an industry-specific level, and data protection is established through rules governing the data involved in specific sectors such as banking and finance, telecommunications, or video rentals.[85] Enforcement is achieved through the imposition of specified civil or criminal sanctions, but there is no agency specifically dedicated to the issue of privacy and/or data protection.[86] While the main advantage of this approach may be the ability to tailor laws to the specific needs of an industry, critics claim that this approach is deficient because it is too reactive and cannot keep up with new technologies or threats to privacy.[87]

Banisar's third category is the "Self-Regulatory Model." In countries that subscribe to this approach, such as Japan and Singapore, the government encourages industry players to develop their own rules and standards. The central criticism of this approach

---

[81] *Id.* at 77 (noting that the framework has also been applied in Canada, Australia, New Zealand, and Hong Kong).

[82] Banisar & Davies, *supra* note 1, at 13 ("This is the preferred model for most countries adopting data protection law.").

[83] Wu, *supra* note 75 (citing the example of a Swedish woman who was fined $450 when she posted the personal information of fellow parishioners in her church group).

[84] Banisar & Davies, *supra* note 1, at 14.

[85] Chik, *supra* note 4, at 77.

[86] *Id.*

[87] Banisar & Davies, *supra* note 1, at 14.

is that it tends to be piecemeal and ineffective due to a lack of incentives for compliance.[88]

The fourth approach, the "Habeas Data Model," only exists in Latin America. Brazil, Paragrauy, Peru, Argentina, Colombia and Costa Rica all subscribe to this model. Chile does not. The Habeas Data Model is also comprehensive in that it covers all kinds of data and does not approach the data protection issue by industry. However, it only applies to information held by the government. Further, it does not generally include a central commission or agency charged with carrying out an information privacy mandate. Instead, the habeas data writ, which literally translates to "you should have the data," grants the individual a constitutional right to petition the constitutional court for access to information. According to Guadamuz, one of the early scholars to write about this kind of data protection regime,[89] "it is designed to protect, by means of an individual complaint presented to a constitutional court, the image, privacy, honour, information self-determination and freedom of information of a person."[90] While the approach has the benefits of other comprehensive legislation - namely that it applies to all types of data and is flexible to changing circumstances and threats to individual privacy - this approach alone fails to provide any infrastructure or support to individuals seeking to exercise their constitutional information rights. In addition, such an approach requires large expenditures on the part of an individual who wishes to access his or her information, since there are no private attorney general incentives incorporated into the scheme.[91]

---

[88] Chik, *supra* note 4, at 77; *see also* Banisar & Davies, *supra* note 1, at 14.

[89] Andres Guadamuz, *Habeas Data: The Latin-American response to Data Protection,* 2 J. INFO. L. & TECH. 1 (2000), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz ("Until now, it is almost impossible to find any literature about Habeas Data outside of Latin America; there is hardly any mention of it even in the most specialised legal publications.").

[90] Andres Guadamuz, *Habeas Data vs the European Data Protection Directive,* 3 J. INFO. L. & TECH. 1 (2001), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz.

[91] Interview with Juan Pablo Olmedo, President of Transparency Council in Santiago, Chile (Jan. 12, 2009).

C. Chile's Privacy Rights Regime: Disappointing in Light of Expectations

Chile's information privacy regime is based on the Comprehensive Model of data protection of Europe, Canada and Australia. However, it fails to enforce many basic information privacy rights to its citizens. What accounts for the disparity?

One might argue that the reason why Chile's data protection regime is weak is because Chile does not maintain a strong comercial presence in the information technology sector. However, a preliminary look at the evidence suggests that no such correlation between information technology investment and stronger privacy protections exists.[92] To appreciate this point, one just has to look to

[92] According to a report published by the *Technology Review* in 2005, the companies with the highest expenditures in research and development in information-heavy industries (computer hardware, computer software, and telecommunications) emanate from eight countries. *See Corporate R&D Scorecard,* TECH. REV., Sept. 2005, *available at* http://www.technologyreview.com/articlefiles/ 2005_rd_ scorecard.pdf. The top-spending companies in information-heavy industries (computer hardware, computer software, and telecommunications) include twelve U.S. companies, six Japanese companies, two German companies, two French companies, one Swedish company, one Finnish company, one British company and one Canadian company. Comparing this information to the 2007 International Privacy Ranking published by Privacy International, a non-profit organization that publishes annual privacy rankings for 47 countries based on a comprehensive list of factors, shows that the seven countries most invested in information-heavy industries maintain widely varying degrees of privacy protections. For instance, the United States, where most of these companies originate, scores 1.5 out of 5. This is the lowest privacy score of the seven countries listed, and is close to the lowest score of the 47 countries monitored by Privacy International (which is 1.3). In contrast, Canada scores 2.9 out of 5. This is the highest of the seven countries listed and is close to the highest score of the 47 countries monitored by Privacy International (which is 3.1). The other countries fall between these two extremes, with Japan scoring 2.2, Germany scoring 2.8, France scoring1.9, Sweden scoring 2.1, and Finland scoring 2.5. Thus, there does not appear to be a correlation between investment in information-heavy industry and the institution of higher or lower privacy protections. *See also Outsourcing Privacy: Countries Processing U.S. Social Security Numbers, Health Information ,Tax Records Lack Fundamental Privacy Safeguards* (September 2005), http://markey. house.gov/docs/privacy/iss_privacy_rep050914.pdf, creating composite privacy rankings for the top 20 countries to which United States citizens' information is likely to be outsourced. The report similarly reflects a wide divergence in privacy

Chile's next-door neighbor, Argentina. In point of fact, the two countries not only share a border over 3,000 miles long, but a number of other salient characteristics. They have a similar history, including a shared Spanish colonial history and similar immigration patterns since independence. Both Argentinean and Chilean populations suffered under dictatorial rule during the 1970s and 1980s, and both autocratic regimes engaged in well-documented human rights abuses. Today, they have similar economic development levels; if anything Chile is more developed.

Argentina's Law for the Protection of Personal Data ("Argentina's Privacy Law"), which went into effect in 2001, is widely lauded as providing exceptionally strong privacy protections.[93] Unlike Chile's Privacy Act, Argentina's Privacy Law created a new privacy body to enforce its provisions and maintain a national registry of databases. It establishes meaningful sanctions for violations, including some criminal sanctions, and empowers data subjects to seek injunctive relief.[94] Pursuant to Article 25 of the EU's Privacy Directive, Argentina's Privacy Law regulates international transfers of data to third countries. In fact, Argentina is the only country in Latin America to be considered by the European Council to have "adequate" data protection laws. Only five other countries in the world have been given this accreditation.[95] Finally, Argentina's Supreme Court recently interpreted Argentina's Privacy Law as providing standing in court not only to an individual data subject,

---

regimes among countries that are likely to process vast amounts of information emanating from the United States.

[93] Salazar, *supra* note 17 at 740 ("It seems that Argentina is perhaps the most 'advanced' in dealing with data privacy and data protection issues."). *See also,* Privacy International, *National Privacy Ranking 2007 – Leading Surveillance Societies Around the World* (2007), *available at* http://www.privacyinternational.org/survey/rankings2007/phrcomp_sort.pdf, ranking Argentina second in privacy protection outside of the European Union, following Canada.

[94] *See* Salazar, *supra* note 17, at 740-41.

[95] This accreditation, part of the EU Directive, is required before EU countries are permitted to send their country's citizens' information to the third country. The other countries to have been given the accreditation are Canada, Switzerland, Guernsey, Isle of Man and Jersey. The United States was not given the accreditation, but negotiated separate "safe harbor" provisions with the EU to maintain trade in information between the two regions.

but also to his brother, in the case of a data subject who had gone missing during Argentina's "dirty war." This suggests that standing to bring suit may be extended one day to groups or classes of individuals.[96]

D. Traditional Explanations for Increased Information Privacy Protections

It stands to reason that, if Argentina has managed to institute strong privacy protections in the last decade, it is all the more likely to expect that Chile would do so as well. What explains the discrepancy between these two countries? Scholars cite three main reasons for strong information privacy protections in a given country: 1) technological advances that increase citizens' vulnerability by exposing them to fraud and abuse, 2) a history of political repression, and 3) pressure from other countries and international organizations.[97]

For the first time in history, vast amounts of data can be aggregated, analyzed, and sent around the world in a matter of seconds. The dramatic increase in computer processing speeds, storage capacities, and networking capabilities in recent decades has provided the potential for misuse of personal information in novel, frightening ways.[98] Opinion polls support the hypothesis that this rise in information technology has led to increased concern about information security.[99] Conversely, those countries that have lagged behind in information technology infrastructure, education and access, are attributed with a lower concern for privacy and data protection values.[100] Thus, "[t[he increasing sophistication of information technology," writes Banisar, "with its capacity to collect,

---

[96] Salazar, *supra* note 17, at 740.

[97] *See, e.g.,* Banisar & Davies, *supra* note 1, at 11-12.

[98] *Id.*

[99] *Id.* at 4 ("Uniformly, populations throughout the world express fears about encroachment on privacy, prompting and unprecedented number of nations to pass laws specifically protecting the privacy of their citizens.").

[100] Alejandra Castro Bonilla, *La protección del derecho a la intimidad en el tratamiento de datos personale: el caso de Espana y la nueva legislación latinoamericana,* 53 AR: REVISTA DE DERECHO INFORMÁTICO 1, 18 (2002).

analyze and disseminate information on individuals introduced a sense of urgency to the demand for privacy legislation."[101]

Another explanation for why some countries may favor strong privacy protections is to remedy past of information privacy abuses under autocratic regimes.[102] This theory is often used to explain why European countries have taken a much stronger stance towards data protection and information privacy laws than the United States: because European countries have the unique experience of suffering beneath dictatorial rule in recent history.[103] Argentina's robust habeas data provisions are also attributed in part to its history of human rights abuses during the "Dirty Wars."[104]

---

[101] Banisar & Davies, *supra* note 1, at 4. Chik posits that increases in information technology concern citizens on three levels: they are concerned about their human rights, their economic security, and their ability to maintain social anonymity. Chik, *supra* note 4, at 67. Other researchers also point to these three core concerns when identifying the anxiety around increased information technology. Holvast notes that an increase in anxiety around information privacy coincided with human rights concerns surrounding racial and gender discrimination, thus augmenting the desirability of maintaining personal information protected. GLOBAL ENCYCLOPEDIA, *supra* note 55. Economic anxiety around increased information technology centers around new potential for the misappropriation of wealth and reputation, such as in the case of identity theft as well as outright use of stolen credit card and bank account information. Finally, new threats to social anonymity are provided as a third explanation of why the rise in information technology results in pleas for more government regulation of data protection. Chik, *supra* note 4, at 55 (arguing that, "online anonymity and the ability to go incognito into the cyber real is a valuable right for the individual").

[102] *See* GLOBAL ENCYCLOPEDIA, *supra* note 55, at 1; Steven R. Salbu, *The European Union Data Privacy Directive and International Relations,* 35 VAND. J. TRANSNAT'L L. 655, 666 (2002) [hereinafter Salbu, *Data Privacy Directive*]; Banisar & Davies, *supra* note 1, at 11; Moshell, *supra* note 70, at 364. *But see* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 YALE L.J. 1151, 1165 (refuting the "dramatic explanation" that European conceptions of privacy are rooted in the European experience with fascism and instead attributing such ideals to older institutional underpinnings, such as feudalism).

[103] GLOBAL ENCYCLOPEDIA, *supra* note 55; *see also* Salbu, *Data Privacy Directive*, *supra* note 102.

[104] Salazar, *supra* note 17, at 740-41 ("Argentineans desire for access to public and private databases was driven in part by their desire to determine the whereabouts of lost family members or to never be denied that information again."). *See also,* Bonilla, *supra* note 100 at 19.

Finally, scholars have shown that countries often adopt strong data protection laws in order to assure compliance or consistency with EU data protection laws.[105] For instance, EU member states were required to pass legislation that was consistent with the EU Directive by 1998. In addition, Article 25(6) of the EU Directive imposes on member states the obligation to ensure that countries with which they share personal information possess an adequate level of data protection.[106] This provides an incentive for countries outside of Europe to bolster their data protection laws in order to receive the accreditation from the EU Council,[107] and creates pressure on countries outside of the EU to enact legislation that is consistent with the EU Directive.[108] Finally, Article 4 extends the jurisdiction of the Directive not only to those companies operating from within member states but also to any companies that make use of data processing "means" or "equipment" in Europe. As a result, virtually any company that collects data on European citizens must also comply with the EU Directive.[109] Even where home countries do not provide for strong data protection regimes, their corporate citizens may be required to follow stringent European-style

---

[105] Banisar & Davies, *supra* note 1, at 11; Moshell, *supra* note 70, at 364.

[106] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L218) art. 25(6). The process by which a non-member state obtains accreditation under 25(6) is lengthy and involved and includes, among other things, an approval by both the national data protection commissioners and the majority of Member States. Once a country has been deemed to provide "adequate" data protection measures, the EU Directive allows data to flow from member states to that country without any further safeguards. *Id.*

[107] The only countries approved thus far are Switzerland, Canada, Argentina, Guernsey, and Isle of Man. The United States has negotiated a separate "safe harbor" agreement with the EU such that data may continue to flow between the two regions, notwithstanding the United States' lack of accreditation as providing an "adequate" level of data protection. European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries* http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

[108] Banisar & Davies, *supra* note 1, at 4.

[109] Wu, *supra* note 75, at 99.

principles nonetheless, paving the way for eventual adoption of stronger information laws in their home countries as well.[110]

E. Applying the Traditional Explanations to the Case of Chile

So are any of these three reasons responsible for Chile's surprisingly weak data protection? The evidence suggests that the answer is no. First, unlike many other developing nations, Chile has been an active participant in the global information technology revolution of the last two decades. According to the World Economic Forum, Chile has the most Internet users, the highest rate of Internet access in schools, and the highest level of access to broadband in Latin America.[111] The Center for Enterprise in Latin America, which has developed the Information Society Indicator to track the progress of Mexico, Brazil, Argentina and Chile in information technology advances over time, consistently ranks Chile the highest among those countries studied.[112] In December of 2006, Chile had 201 computers and 294 Internet users per 1000 inhabitants.[113]

Second, Chile, like many European countries, also has a recent history of dictatorship. General Augusto Pinochet took control of the country in 1973 via a bloody military coup and stayed in power absent a democratic mandate until 1990. Countless human rights abuses took place under the rule of Pinochet, including information privacy abuses.[114] In fact, remnants of Pinochet's abusive regime exist to this day. For instance, the Investigations Police still keep records of all adult citizens and issue ID cards that must be kept at all times.[115]

---

[110] *See id.* at 104 ("There's been a complicated shift, making the EU the most influential voice in global privacy regulation, in part because it seems to care the most.").

[111] WORLD ECONOMIC FORUM, GLOBAL COMPETITIVENESS REPORT 2008-2009 (2009), available at http://www.weforum.org/documents/GCR0809/index.html.

[112] EVERIS, INDICADOR DE LA SOCIEDAD DE INFORMACIÓN (ISI): SITUACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN ARGENTINA, BRASIL, CHILE Y MEXICO 10 (2006).

[113] *Id.* at 32. Chile also had 713 cell phones per 1000 inhabitants, which is almost as many as the United States, according to the study. *Id.*

[114] *See, e.g.*, Christine Sypnowich, *The Civility of Law: Between Public and Private, in* PUBLIC AND PRIVATE, LEGAL POLITICAL AND PHILOSOPHICAL PERSPECTIVES, 84, 99 (2000).

[115] Banisar & Davies, *supra* note 1, at 30-31.

There is also evidence that the personal data compiled during the military regime was never destroyed.[116] As recently as 1998, Pinochet threatened to use "compromising information," collected during his regime, against those who were trying to keep him from achieving the position of senator for life.[117] Thus, it would seem that Chile has the same motivation as many other European countries that suffered abuses under dictatorial rule to modify its legal system to prevent abuses of information privacy in the future.

Third, and finally, Chile's relationship with Europe is significant. If one of the reasons why countries adopt strong data protection regimes is to acquiesce to pressures induced by strong trade with the European Union, one would imagine that Chile would face the same pressure. As of 2007, 23.9% of Chile's total exports went to the European Union.[118] The EU's share of Chile's total imports was 13.8%.[119] In fact, the EU is Chile's main trade partner and main export partner, accounting for a greater percentage of Chile's total trade and exports than both the United States and China.[120] The EU is Chile's second major import partner, preceded only by the United States.[121] In other words, if pressure from the EU is a significant factor in determining whether a country is likely to have strong privacy protections, one would think that Chile would be subject to such pressure given its strong economic dependence on the region. This suggests that there must be a fourth factor that, combined with the traditional three factors, explains the variation in privacy regimes across the world. That fourth factor is culture.

III. POLITICAL AND CULTURAL EXPLANATIONS FOR CHILE'S RELATIVELY WEAK INFORMATION PRIVACY REGIME

Steven Salbu writes, "[W]hile the ideal of a normative global village may be enticing, and while we are likely moving in this

---

[116] *Id.* at 31.
[117] *Id.*
[118] EUROPEAN COMMISSION, CHILE – TRADE STATISTICS (Sep. 15, 2008), http://trade.ec.europa.eu/doclib/cfm/doclib_section.cfm?sec=119&lev=2&order=date, 4.
[119] *Id.*
[120] *Id.*
[121] *Id.* at 6.

direction, the current condition of the world hardly comprises a single community with a single culture of common norms, beliefs, and values."[122] If culture influences the degree to which a country's data protection regime adequately protects information privacy, one would expect that political cultures that prioritize alternative values above privacy will be lax when it comes to enforcing data protection laws. The case of Chile supports such a hypothesis. Chile's success with radical free market policies in the latter half of the twentieth century, combined with its experience under harsh dictatorial rule, has resulted in a political culture that values the free flow of information and freedom of expression over continental-style privacy values. In turn, Chile's data protection regime is demonstrably weaker compared to data protection regimes in Europe.

A. Theoretical framework

In the late 1970s and early 1980s, the Dutch social psychologist, Geert Hofstede conducted hundreds of interviews with IBM employees from over 53 countries.[123] Because every individual in the sample belonged to the same corporate culture, Hofstede was able to observe variance across national cultures.[124] Hofstede found four central dimensions upon which cultures varied significantly: power-distance, individualism/collectivism, femininity/masculinity, and uncertainty avoidance.[125] Across these dimensions, Hofstede found significant variation among countries,[126] as well as among regions.[127]

---

[122] Steven R. Salbu, *Are Extraterritorial Restrictions on Bribery a Viable and Desirable International Policy Goal Under the Global Conditions of the Late Twentieth Century?*, 24 YALE J. INT'L L. 223, 230 (1999) [hereinafter Salbu, *Extraterritorial Restrictions*].

[123] *See* HOFSTEDE, *supra* note 11.

[124] *But see*, JULIE A. JACKO & ANDREW SEARS, THE COMPUTER-HUMAN INTERACTION HANDBOOK: FUNDAMENTALS, EVOLVING TECHNOLOGIES AND EMERGING APPLICATIONS (CRC Press, 2003).

[125] *See generally* HOFSTEDE, *supra* note 11.

[126] Hofstede found that where participants from the United States exhibited the highest level of individualism, participants from Chile ranked 38 out of 53. Hofstede defines individualism as pertaining to "societies in which the ties between individuals are loose: everyone is expected to look after himself or herself and his or her immediate family. Collectivism as its opposite pertains to societies in which people from birth onward are integrated into strong, cohesive in-groups, which throughout

Significant differences in cultural norms have also been found with respect to privacy in particular. James Whitman has identified two different cultural conceptions of privacy in the Western world: the dignity perspective and the liberty perspective.[128] He argues that privacy values are culture-specific, so that "[w]e do not seems to posses general 'human' intuitions about the 'horror' of privacy violations. We possess something more complicated than that: we possess American intuitions - or, as the case may be, Dutch, Italian, French or German intuitions." [129]

Or, as the case may be, Chilean intuitions. Renato Jijena, who has written extensively on the Chilean data protection regime, notes that "[t]he legal protection of personal data is a judicial topic that is given a lot of perspective overseas, but in our country the reality is that it is unknown and little studied."[130] Similarly, Rodolfo Herrera Bravo writes that, "even though Chile has a specific norm that, supposedly, protects natural persons from the treatment of their [personal] data . . . this topic is still pending because, in our opinion, there is a lack of adequate information to create a consciousness about the enormous importance that it has."[131] Thus, while a handful

---

people's lifetimes continue to protect them in exchange for unquestioning loyalty." *Id.*

[127] When scores were normalized from 0 to 100, the average individualism score for Latin American countries was 21 and the median score was 16. In contrast, the average individualism score for EU countries was 64.6 and the median score was 70.5. The Latin American countries (and their scores) in the sample were: Argentina (46), Brazil (38), Chile (23), Colombia (13), Costa Rica (15), Ecuador (8), Guatemala (6), Mexico (30), Panama (11), Peru (16), Salvador (19), Uruguay (36), and Venezuela (12). The European Union countries (and their scores) in the sample were: Austria (55), Belgium (75), Denmark (74), Finland (63), France (71), Germany (67), Great Britain (89), Greece (35), Ireland (70), Italy (76), Netherlands (80), Portugal (27), Spain (51), and Sweden (71). *Id.*

[128] *See generally*, Whitman, *supra* note 102, at 1160-1161.

[129] Whitman, *supra* note 102, at 1160.

[130] RENATO JIJENA LEIVA, COMERCIO ELETRÓNICO, FIRMA DIGITAL Y DERECHO: ANÁLISIS DE LA LEY NO. 19,799, at 76 (Editorial Jurídica 2d ed. 2005) (author's translation).

[131] Herrera Bravo, Rodolfo, *La Protección de Datos Personales como Garantía Básica de los Derechos Fundamentales,"* 2(5) REVISTA DE DERECHO PÚBLICO DE LA AGRUPACIÓN DE ABOGADOS DE LA CONTRALORÍA GENERAL DE LA REPUBLICA 83 (2001) (author's translation). *See also,* ANGUITA, *supra* note 35, at 251 (noting that

of Chilean scholars clamor for greater awareness about information privacy, there do not appear to be cultural norms that support even a debate on the topic at the present time.

B. Chilean Culture: Weighing Trade-Offs

A high degree of privacy protection necessarily entails that competing and perhaps equally salient values must take a back seat. These values include innovation, efficient production and distribution, access to cheaper goods and services (especially for the poor), simplicity, functionality, free speech, reduced debt through better screening processes, better debt collection efforts, access to services for the handicapped and elderly, assistance to law enforcement, and reduction of fraud.[132]

1. Access to Information

Countries that place a high value on privacy norms will forfeit some degree of access to information in return for more privacy, and vice versa. Chile and Europe are a study in great contrast regarding their political culture. Whitman explains that Europe, by deciding to eschew the free flow of information regarding financial transactions, has not been able to develop credit markets as effectively as one would predict based solely on the size of its market and level of economic development. Whitman explains:

> For the continental legal tradition the basic issue is of course not just one of market efficiency. Consumers need more than credit. They need dignity. The idea that any random merchant might have access to the 'image' of your financial history is simply too

---

when the Privacy Act bill was debated in Congress, very few doctoral dissertations on issues of privacy existed in Chile).

[132] *See* Symposium, *Panel II, The Conflict Between Commercial Speech and Legislation Governing the Commercialization of Private Sector Data, in Data Privacy Laws and the First Amendment: A Conflict?*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 59, 66 (2000).

> intuitively distasteful to people brought up in the continental world.[133]

In contrast, Fuentes and Maquieira found that information sharing was one of the factors that had a significant positive effect on the availability of bank loans in Chile because it indicated the ability of banks to share information about customers that, in turn, helped provide citizens with access to credit.[134]

Chilean citizens value access to information and free expression, not information privacy. This cultural predisposition has deep roots bolstered by Chile's recent history. Chile has the distinction of having one of Latin America's oldest democratic traditions. This tradition, however, was punctuated by a repressive dictatorship between 1973 and 1989. Indeed, this authoritarian regime introduced a brand of neo-liberal free market economics under General Augusto Pinochet that significantly shifted Chilean attitudes, from relatively socialist values to relatively capitalist ones.[135] The support of free and efficient markets is now valued highly in Chile. In turn, free and easy access to information has become a central tenet of Chilean political culture.[136]

---

[133] Whitman, *supra* note 102, at 1192. *See also*, Federico Ferretti, *The Legal Standing of Consumer Credit Reporting in the European Community,* 123(9) BANKING L.J. 835 (showing that the data protection directive regulates consumer credit in Europe).

[134] J. Rodrigo Fuentes & Carlos Maquieira, *Institutional Arrangements to Determine Loan Repayment in Chile* 1(Inter-American Development Bank, Working Paper No. R-374,1999).

[135] *See generally* JAVIER MARTÍNEZ BENGOA & ALVARO H. DÍAZ PÉREZ, CHILE, THE GREAT TRANSFORMATION ix (Brookings Institution Press 1996); JUAN GABRIEL VALDÉZ, PINOCHET'S ECONOMISTS: THE CHICAGO BOYS IN CHILE (Cambridge University Press 1995).

[136] *See generally,* Kevin Cowan & José de Gregorio, *Credit Information and Market Performance: the case of Chile, in* CREDIT REPORTING SYSTEMS AND THE INTERNATIONAL ECONOMY (Margaret J. Miller ed., 2003) (summarizing literature on the positive correlation between information sharing and various indicators of access to credit).

2. Freedom of Expression

Another salient value for which privacy is traded is freedom of expression.[137] Indeed, Warren and Brandeis's seminal work, *The Right to Privacy* was partially motivated by what the authors viewed as "press incursions" into their personal privacy.[138] The article "was written in a fit of outrage over newspaper reports of a party given by the Warrens, and its main target was the gossip pages of the 'yellow press,' which Warren and Brandeis were convinced represented a new phenomenon."[139] While the United States' failure to adopt stringent data protection policies vis-à-vis Europe has been attributed to the high value Americans place on freedom of expression,[140] this cultural trait is not unique to the United States.

Chile has a violent history of repression of speech under Pinochet and the military regime.[141] As described in a 1998 report issued by Human Rights Watch: "the regime used virtually every method in the censor's repertoire: prior censorship of news and opinion, the banning of films for ideological reasons, concoction and dissemination of false information, impounding of publications, closures, the enforcement of draconian national security laws, harassment and intimidation."[142] Twenty-three journalists were killed or "disappeared" under the regime.[143] In the first two years of the dictatorship, 400 journalists lost their jobs, 200 had left the country and fourteen were put in jail.[144] This dramatic repression of free expression has resulted in cultural values that place more emphasis on free expression than privacy. Paradoxically, therefore, the Chilean

---

[137] *See generally id.*

[138] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[139] Whitman, *supra* note 102, at 1204.

[140] *Id.* at 1209 ("Freedom of expression has been the most deadly enemy of continental-style privacy in America.")

[141] *See* HUMAN RIGHTS WATCH, LIMITS OF TOLERANCE: FREEDOM OF EXPRESSION AND THE PUBLIC DEBATE IN CHILE 28 (1998) ("The onslaught on press freedoms and the repression of political dissent in the aftermath of the military coup were harsher, more drastic and sweeping, than anything seen before in Chilean history.").

[142] *Id.* at 28-29.

[143] *Id.* at 29.

[144] *Id.*

case may be one where a history of dictatorship contributed to *weaker* privacy protection.

Support for this thesis can be extracted from the enactment of recent legislation regarding transparency in government. In July of 2008, Chile passed new transparency legislation (the "Transparency Law") that significantly increased access to public information and information regarding the administration of the state.[145] In the last legislative session, two parliamentarians made an eleventh-hour change to section 33 of the Law, which outlines the responsibilities of the newly-created Council for Transparency. The change was codified in the final version of the bill as provision 33(m). This provision charges the Council for Transparency with executing the provisions of the Privacy Act.[146] Although the law is twenty-seven pages long, the provision on privacy is a mere three lines, attesting to the hierarchy of Chile's political cultural values: privacy protection plays second fiddle to freedom of speech.

C. Alternative Explanations for Chile's Weak Information Privacy Protections

If Chile's political culture is an important determinant of its surprisingly weak privacy protection regime, what alternative factors may also explain this outcome? How do they stack up against political culture?

There are three main counterarguments to the thesis that culture explains Chile's relatively weak information privacy regime. The first counterargument is that the failure to enact a robust data protection regime is really a failure of democracy – that Chile lacks the institutional infrastructure necessary to implement a European-style comprehensive model information privacy system. The second

---

[145] Transparencia de la Función Pública y de Accesso a la Información e la Administración del Estado, [Transparency of the Public Sector and Access to Information and to the Administration of the State], Law No. 20285, Agosto 20, 2008, DIARIO OFICIAL [D.O.].

[146] *Id.* art. 33(m) ("Velar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado." ["Provide for the adequate compliance with Law No. 19628, regarding the protection of personal data, on the part of the bodies of State Administration."]) (author's translation).

counterargument is that the failure to enact strong data protection laws is simply a collective action problem – that dispersed individuals who value information privacy are no match for powerful corporate interests that can lobby government with a single voice. Finally, the third counterargument is that Chile's Privacy Act has nothing to do with human rights based conceptions of privacy – rather, it was a law passed to ensure liquidity in the credit markets and, unsurprisingly, the law fails to do much else. None of these arguments, however, can fully explain the discrepancy between Chile's data protection regime and those in Europe or Argentina as well as culture can.

1. The Institutional Hypothesis

The first competing hypothesis to the culture argument is that Chile's weak information privacy regime really represents a failure of democracy. Under this theory, Chile's democratic institutions simply aren't as robust as those in the U.S. and Europe (or Argentina), which is why the data collection lobby was able to keep citizens out of the debate over the Privacy Act. This idea is simply not borne out in the evidence. Chile's democratic process, as measured by various indicators, is higher than the Latin American average, higher or equal to the Argentinean levels, and close to European levels.[147] Moreover, unlike most Latin American countries, Chile was a democracy for the vast majority of the twentieth century. Finally, there is a large consensus among Chilean privacy scholars that information privacy is not and has never been a part of the larger public debate in Chile.[148] Thus, even if there were significant problems with Chile's democratic institutions, there do not appear to be voices clamoring for data protection legislation that are being kept out of the discussion. A failure of democracy does not explain the lack of those voices – rather, culture does.

---

[147] *See* Stephen Haber, *Latin America's Quiet Revolution*, THE WALL STREET JOURNAL, Jan. 30, 2009, at W3.

[148] *See* ANGUITA, *supra* note 35; Jijena, *supra* note 130.

2. The Collective Action Hypothesis

The second hypothesis is that the reason for Chile's relatively weak data protection regime can be explained by a classic collective action problem: dispersed individuals and consumers who value their privacy don't care as much as the highly concentrated handful of information collection companies care about maintaining their access to that information.[149] But if this is the only explanation for Chile's weaker data protection laws, why don't other nations face the same problem? Aren't all countries that attempt to enact information privacy subject to identical constraints? Yet, other nations – including other very similar nations, such as Argentina – have been able to overcome these barriers. Thus, the issue reverts to the question of what makes Chile different than those countries that have been able to overcome the collective action problem. The answer is culture.

3. The Credit Market Hypothesis

The third counterargument against the political culture hypothesis is that the real reason for Chile's inadequate data protection legislation is that it was created primarily to bolster the country's credit market. As such, provisions in the Privacy Act that relate to non-financial information were either not given the attention required to adequately protect such personal information, or Congress was captured by the information collection industry, which had a vested interest in blocking information privacy.[150]

This "Credit Market Theory" is rooted in the unique history of Chile's credit market, originating in the economic policies enacted by the Pinochet dictatorship during the 1970s. These neo-liberal policies, which included large-scale deregulation and privatization, also included the transformation of Chile's small, informal credit market into a modern, vibrant credit market. This so-called

---

[149] *See, e.g.*, Chik, *supra* note 4, at 76.

[150] Asia is also a region that has purportedly chosen to forgo strong data protection in light of countervailing factors. *See* Chik, *supra* note 4, at 62. The story of Chile is different than the story of Asia though. In Asia, ostensibly the concern is for preventing the obstruction of lucrative IT business in the region through the passage of overly restrictive privacy laws. In Chile, however, the design was not to promote the growth of IT services of data collection companies, but to allow them to function because their credit markets had become reliant on them.

"democratization of credit" granted citizens access to cheap credit; in turn, this significantly broadened the market for credit and fueled a credit bubble.[151]

In 1983, the bubble popped, and a credit crisis ensued causing many banks to fail. Unemployment skyrocketed in the wake of the crisis and citizens began to default on their debts, and their information began to populate debtor databases run by both the government and private agencies.[152] Most employers then began to require commercial certificates that documented prospective employees' credit histories, which had the effect of blackballing indebted individuals and those who had defaulted on their loans. This practice worsened the economic crisis because it exacerbated unemployment and, ultimately, protracted a credit crunch triggered by the predictable retrenchment of loans as banks sought to shore up their balance sheets.

The Credit Market Theory views Chile's Privacy Act as a delayed response to this credit market failure. Policy-makers believed that data protection was required to avoid repeating the mistakes that undergirded an unrelenting credit crunch that persisted well into the late 1980s. If government agencies and private information gatherers were forced to purge credit history databases after the passage of a reasonable amount of time, citizens who had run into credit trouble in the past would not be barred from re-entering and hence re-invigorating the credit market. Shortly after democracy was reinstated in Chile, Congress finally passed the privacy legislation and provisions relating to non-financial information only as an afterthought.[153]

---

[151] ANGUITA, *supra* note 35.

[152] *See Id.* at 224.

[153] Axel Buchheister noted that the enforcement of contracts in Chile is weak in comparison to other countries with similar economies. As a result, the credit market is far more dependent on historical financial information about individuals and companies than it would otherwise be. Interview with Axel Buchheister R., Director of Legal Studies, Libertad y Desarollo, (Jan. 16, 2009). *See also* Cowan & de Gregorio, *supra* note 136, 172 (showing that Chile has some of the lowest rates of nonperforming loans in the world and one of the largest banking sectors in the developing world).

While the Credit Market Theory is compelling, it does not explain why Chile's data protection law is weaker than similar laws in other countries. While the theory explains why there may have been a desire in Chile to pass a law that protected financial information to prop up the credit market, it does *not* adequately explain the absence of the desire to pass a law that protected personal information of other kinds. Provided that the Privacy Act also addresses non-financial personal information, why was this part of the law not made stronger? After all, strengthening protections for non-financial information would not have weakened privacy protections for non-financial information.

The truth is that a few voices from consumer groups or civil liberties organizations influenced debate in Congress over the Privacy Act. During the six years that the Privacy Act was deliberated, the only constituency that really lobbied Congress was the information collection industry.[154] Indeed, this lobbying effort began in earnest before the bill that became the Privacy Act was introduced in Congress. Between 1986 and 1987, three privacy related initiatives were tabled; however, they never made it passed the proposal phase. These proposals, developed in consultation with the information industry, defined freedom of information as "the right to use and make use of the procedures with which one can legally collect, process, store, transmit and divulge data."[155] Clearly, the concern here was to preserve the rights of data processors, not data subjects.[156]

The piece of legislation that eventually became Chile's Privacy Act started as a bill in the Senate in 1993 and was only approved by a Mixed Committee in October of 1999.[157] The first report from the Senate's Commission on the Constitution, Legislation, Justice and Senate Regulation included papers written by professors and commissioned by credit rating and direct marketing agencies. Thereafter, there is no evidence of significant participation

---

[154] ANGUITA, *supra* note 35, at 225.
[155] *Id.* at 225-27 (author's translation).
[156] The first bill brought to the floor after democratic reform in 1991 included almost the exact same text as the bill proposed under the military regime. *Id.* at 227.
[157] *Id.* at 233.

of any group outside of the information collection industry.[158] So does this evince a civil society vacuum in Chile, where citizen groups organized around civil liberties and human rights issues simply do not exist?

In fact, the opposite is true. Human rights organizations, think tanks, and other elements of a vibrant civil society began to develop in the late stages of the Pinochet dictatorship in order to support a transition to democracy.[159] Since the transition occurred, these groups have maintained powerful influence over Chilean policy-makers, and frequently lobby Congress.[160] Thus, the absence of civil society in the information privacy debate cannot be attributed to a lack or underdevelopment of such groups in Chile generally.

In short, while shoring up the credit market may have indeed mattered for enacting the Privacy Act, this does not explain why Chilean citizens did not clamor for more protection of their personal information.[161] After all, the rise in information technology, a history of dictatorship, and pressure from the EU seemed to foretell greater grassroots involvement by citizens concerned over their right to privacy.

Anguita notes that there was an "absence of previous public reflection and discussion, and, more generally - which to this date has not occurred in Chilean society - about the effects and incidence of new technology, especially information technology, on privacy or the private life of people, something that necessarily should have driven and inspired the legislative policy."[162] The most compelling explanation for this lack of participation and debate is culture:

---

[158] *Id.* at 249.

[159] *See also* Civicus: World Alliance for Citizen Participation, *Chile: The Associational Reconstruction of a Nation,* CIVIL SOCIETY INDEX REPORT FOR CHILE, http://www.civicus.org/new/media/CSI_Chile_Country_Report.pdf. *See generally,* EXPLORING CIVIL SOCIETY: POLITICAL AND CULTURAL CONTEXT (Marlies Glasius et al. eds., Routledge 2004).

[160] *See generally,* EXPLORING CIVIL SOCIETY: POLITICAL AND CULTURAL CONTEXT (Marlies Glasius et al. eds., Routledge 2004).

[161] Indeed, given that citizens were deeply affected by the status quo – unable to work and unable to borrow – one would think that a great deal of clamoring for data protection would have taken place.

[162] ANGUITA, *supra* note 35, at 234 (author's translation).

Chileans simply do not value privacy that highly as compared to other countries.

IV. IMPLICATIONS

The idea that culture may have played a significant role in determining the strength of Chile's data protection law has several implications that reach beyond Chile's sinewy borders. First, to the extent that other Latin American cultures embrace a similar conception of privacy as Chile, we should expect that these countries will have similarly weak information privacy regimes. In addition, recognizing that culture may affect the level of information privacy available within a country also means that as developing countries continue to participate more fully in the information technology revolution of the last two decades, this does not mean that they will automatically embrace strict privacy regimes like those that exist in Europe. Moreover, even countries that have suffered abuses under autocratic regimes, and those countries faced with implicit pressure from the international community to adopt more protective data protection measures, will not necessarily do so if there is no political culture of privacy.

Thus, the most critical implication of recognizing culture as a determinant of data protection regime strength is that harmonization efforts in the area of privacy law, such as the EU Directive, may experience reduced efficacy once extraterritorial reach extends into countries with vastly different cultural conceptions of privacy.[163] If Chile is any indication, this is likely to be the case in Latin America, with the exception of Argentina.

Therefore, even if countries that value privacy differently than Europe adopt European-style data protection laws, recognizing the role of culture in the implementation of those laws lends support

---

[163] *See, e.g.*, BENGOA & PÉREZ, *supra* note 135 (making a similar argument with respect to countries attempting to replicate the successful economic policies of Chile and noting that "since the resource endowments, cultures, demographics, and economic and political systems of these countries may differ markedly from those of Chile, there is no reason to expect that transplanted policies will produce a standard result"); *See also* OSCAR G. CHASE, LAW, CULTURE & RITUAL 48 (N.Y. Univ. Press 2005) ("Any proposal to borrow from another society should prompt a cultural inquiry.").

to theorists who conclude that there is a great danger that the execution of such laws will differ dramatically.[164] This is what occurred in Chile, where a Comprehensive Model law was adopted yet failed to incorporate the elements that would allow for effective protection of personal data. Beyond the case of Chile, this pattern has already been shown to be at work in the area of privacy legislation. Studies demonstrate that countries that have adopted privacy laws that derive from the first principles articulated in the OECD Guidelines and other instruments often diverge in the execution of those principles.[165]

The question then is, if countries are not going to enact strong data protection laws on their own, should developed countries use more coercive tactics – either through the market or otherwise – to force them to do so? Some might argue yes: where countries and economies are increasingly connected through technology and the internet, failure to harmonize privacy standards may create incentives for dangerous information privacy abuses. And these abuses will affect citizens everywhere, even in those countries that have chosen to make the trade-offs necessary to enact a strong data protection regime in their home country.[166] On the other hand, as some have pointed out with respect to extraterritorial anti-corruption laws, "[t]he peril of extraterritorial application is the risk of inflicting incongruent or discordant values on others in instances where legitimate, nuanced moral differences are supportable."[167]

Regardless of the outcome of this debate, recognizing the effect that culture has on privacy policy suggests that harmonization efforts will likely not take naturally once a given country has reached some set of benchmarks. Rather, there is likely to be resistance to policies that create trade-offs that do not accord with cultural values.[168] When political culture is included in the equation, there is

---

[164] *See, e.g.*, Reidenberg, *supra* note 73, at 1330.

[165] *See* Reidenberg, *supra* note 73, at 1330.

[166] *Id.* ("The danger is that seemingly small differences can have significant effects as obstacles to online services or as incentives for the distortion of services.").

[167] Salbu, *Extraterritorial Restrictions*, *supra* note 122, at 231.

[168] *See* Salbu, *Data Privacy Directive*, supra note 102, at 689 ("Approaches that are consistent with a nation's culture and interests will be highly valued, and efforts to thwart these approaches can be threatening.").

no sidestepping the fact that tolerance and privacy are on a collision course.