WHITE & CASE

International Data Protection and Privacy Law

August 2009

§ 24:1 International Corporate Practice and Data Privacy Law

§ 24:2 European Union Data Privacy Directive and European Data Privacy Law

§ 24:2.1 Scope of EU Data Directive

§ 24:2.2 Social and Legal Context Underlying EU Data Directive

§ 24:2.3 Definitions

§ 24:2.4 Processing Data Domestically in Europe

[A] Complying with Data Quality Principles and Rules

[B] Disclosure of Processing to Data Subjects

[C] Reporting Data Processing to Data Protection Authorities

§ 24:3 Transfers of Personal Data Outside Europe

§ 24:3.1 Data Transfers to Countries with "Adequate" Data Protection

§ 24:3.2 Safe Harbor

[A] Seven Safe Harbor Principles

[A][1] Notice

[A][2] Choice

[A][3] Onward Transfer

[A][4] Security

[A][5] Data Integrity

[A][6] Access

[A][7] Enforcement

[B] Safe Harbor's Self-Certification Process

[C] Criticisms of Safe Harbor

§ 24:3.3 Binding/Standard/Model Contractual Clauses

[A] Obligations of the Data Exporter and Data Importer

[B] Apportionment of Liability

§ 24:3.4 Binding Corporate Rules

§ 24:4 "Transposition" of the EU Directive in Selected European States

§ 24:4.1 Denmark

§ 24:4.2 England

§ 24:4.3 France

§ 24:4.4 Germany

§ 24:4.5 Italy

§ 24:4.6 Netherlands

§ 24:4.7 Switzerland

§ 24:5 Data Privacy Laws Beyond Europe

§ 24:5.1 Argentina

§ 24:5.2 Australia

§ 24:5.3 Brazil

§ 24:5.4 Canada

§ 24:5.5 China

Donald C. Dowling, Jr.

White & Case

This article was published in slightly different format as Chapter 24 in the Practising Law Institute treatise *International Corporate Practice*.

§ 24:5.6 Colombia

§ 24:5.7 Costa Rica

§ 24:5.8 Hong Kong

§ 24:5.9 India

§ 24:5.10 Israel

§ 24:5.11 Japan

§ 24:5.12 Mexico

§ 24:5.13 Russia

§ 24:5.14 Singapore

§ 24:5.15 South Korea

§ 24:5.16 Taiwan

§ 24:5.17 Thailand

§ 24:5.18 Uruguay

§ 24:1 International Corporate Practice and Data Privacy Law

Of all the branches of international corporate law practice, perhaps the one that has most recently emerged as a key part of practice is international data privacy law. Before the late 1990s, data privacy was comprehensively regulated only in a few countries, and those few data laws had mostly local effects, rarely catching the attention of compliance officers at corporate headquarters.

But compliance with foreign data privacy laws has now become hugely important for multinational headquarters. Here are the top five reasons why:

1. Extraterritorial Reach. While data laws have profound local effects, many of these laws restrict data transmissions abroad (as they must, to regulate noncompliance offshore), and are to that extent inherently cross-border.

2. Knowledge Economy. Many businesses these days traffic in data. The broad definition of "data processing" under data laws picks up much of the core customer business functions in sectors such as financial services, insurance, consulting, journalism, and many others. Even multinationals in manufacturing and other less data-intensive fields need sophisticated human resources information systems and customer management platforms from vendors like PeopleSoft, Oracle, SAP, and Ceridian.

3. Penalties. Penalties for violating data laws can be significant, especially in Europe and Canada. By law, European "data subjects" have a private right of action for data law violations. Separately, every European country has a dedicated data agency to enforce data laws. These agencies are getting vigilant. For example, Spain's data agency—said to be self-funded from the fines it collects—can impose fines up to €600,000, and in recent years has imposed a number of €300,506 fines for illegal data transfers. France's cap on fines is €150,000 for a first offense, plus five years in prison. German data fines can reach €250,000. In the United Kingdom, fines are unlimited. Further, in 2007, the United Kingdom took steps to amend its data law to add a penalty of two years in prison for unauthorized data disclosures.

4. Publicity. Violating data privacy law imposes costs beyond the penalties. In Europe especially, citizens jealously guard their privacy, and so any multinational caught flouting privacy rights can suffer a significant public relations hit. In Europe, news of a data privacy law violation can have an effect similar to news stateside of a breach of sex harassment laws. (For that matter, even in the United States, companies guilty of domestic data breaches now encounter serious P.R. problems.)

5. Tougher Regulations Abroad. While laws on every topic differ from country to country, laws in many areas covered in this book tend to be at least as strict in the United States as abroad—for example, think of laws on securities, corporate governance, accounting standards, tax, antibribery, money laundering, migration, export controls, environmental law, and bankruptcy. Not so data privacy. While the United States has an intricate web of laws that touch on various specific aspects of data privacy, it has nothing like the comprehensive data privacy regulatory regime imposed in jurisdictions as varied at the European Union and the European Economic Area, Canada, Argentina, Hong Kong, and Australia. Indeed, companies' US multinational headquarters, when confronted for the first time with advice on foreign data privacy laws, is often in disbelief or denial: "Surely those countries don't impose laws so business unfriendly as that! How on earth are we supposed to operate under rules that strict?"

This final point, on the difference between US privacy regulation and the omnibus data protection laws in foreign countries, in large part relates to the jurisprudential gulf separating the American "sectoral"

approach to privacy regulation from other countries' comprehensive approach. This is in essence the difference between US free speech and the foreign focus on personal confidentiality. The First Amendment to the US Constitution guarantees that "Congress [and the state and local governments, via the Fourteenth Amendment] shall make no law . . . abridging the freedom of speech, or of the press. . . ." Of course, the most interesting topic of speech and the press is always *people*. Because the First Amendment grants us an explicit right to discuss, print, or post online most information we have about others—without any express exception for speech that might intrude on someone's claimed privacy— the text of the First Amendment elevates free speech interests above privacy concerns. As such, the Constitution actually protects would-be privacy violators more explicitly than potential victims of privacy breaches: Our free-speech right is *explicit*, but our privacy right is merely *implicit*. Unlike many other countries' constitutions, the US Constitution nowhere contains the word "privacy"; in fact, the privacy right, according to the Supreme Court, exists only in the Constitutional "penumbra," or shadows.

Meanwhile, Europe, Canada, Argentina, and other jurisdictions with constitutional privacy protection and comprehensive data protection laws come at this issue from an entirely different perspective. Rather than putting privacy interests on a scale counterbalanced by free speech rights, these countries analogize privacy rights with intellectual property rights. Just as intellectual property is data belonging to an owner, these countries' legal systems protect personal data almost as *belonging* to the person whom it is about. Why should an individual citizen's political affiliation, salary, and sexual orientation be less worthy of property protection than a for-profit business's trademark, slogan, and jingle? If government is going to let corporations keep competitors from exploiting brand names and trademarks, the law certainly should let a citizen keep others from trafficking in his credit history and sex life.

The difference between these approaches is even greater in nations that suffered under fascist governments during and after World War II, where secret police exploited personal information in classified files for nefarious government purposes—such as selecting whom to send off to concentration camps. This legacy in these countries instills a healthy skepticism of governments (and, for that matter, faceless corporations) amassing data banks with personal information used for who-knows-what purposes.

In the eyes of many privacy advocates, the European approach to privacy regulation seems defensible—indeed, preferable. But it obviously raises a fundamental conflict in the United States. The European approach in effect prioritizes privacy over free speech, while the US in effect does the reverse.

This chapter offers an overview of foreign data protection law systems, focusing on a detailed analysis of the world's most important comprehensive data protection legislation, that of the European Union and its member states. The chapter then touches on data protection laws outside Europe, including in some nations with data laws patterned on, or influenced by, the European system.

§ 24:2 European Union Data Privacy Directive and European Data Privacy Law

In 1995, the Brussels-based European Union (EU) passed a comprehensive data privacy law called the "European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data."[1] The legislative tool the EU selected for privacy law—the "directive"—requires each EU member state (of which there are now twenty-seven)[2] to enact its own local law adopting (or "transposing") the thrust of the directive. The EU data Directive mandated that the member states pass their local data laws by October 25, 1998, but in fact full implementation took several years more.[3]

Therefore, the text of the EU data Directive offers us a blueprint for data privacy laws across Europe, but in any given situation, the Directive itself is merely a framework. As to each specific data privacy issue arising within Europe, the statute of the relevant

1. EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. L 281 [hereinafter "Directive"].

2. As of 2007, the European Union consists of 27 member states: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

3. Directive, ch. I, art. 4 (discussing Member states' adoption of national provisions). For a discussion of member-state adoption of the Directive, by this author, *see, e.g.,* Donald C. Dowling, Jr., Preparing To Resolve US- Based Employers' Disputes Under Europe's New Data Privacy Law, 2 J. ALT. DISP. RESOL. IN EMP. no. 1 at 31 (Spring 2000), reprinted at 1 ALSB INT'L BUS. L.J. 39 (2000), *available at* www.alsb.org/international/ijrnl/ dowling/text.htm.

country or countries that adopts ("transposes") the Directive will determine data privacy rights and responsibilities.[4] In other words, the Directive itself speaks only to the twenty-seven member state governments. For most purposes, it does not itself dictate rights of European individuals or companies. But it does serve as a framework for discussing data protection laws across Europe.[5]

§ 24:2.1 Scope of EU Data Directive

The EU data Directive requires each member state to pass a privacy law, called a "data protection" law, that reaches both government and private entities—including businesses that process employee and consumer data. While America's "sectoral" privacy laws target discrete categories of data (medical and credit records, children online, etc.), the Directive mandates omnibus laws that cover *all* "processing" (defined to include even collection and storage) of data about personally identifiable individuals. The Directive is not anchored to electronic (computerized) data, and therefore reaches written, Internet, and even oral communications. Plus, its sweep goes well beyond business data. Read broadly, the Directive could reach, for example, even private and mundane communications like a love letter or a gossipy chat between friends.[6]

An important aspect of the EU data Directive for businesses based outside of Europe, such as in the United States, is the law's extraterritorial reach. Because it would otherwise be so easy to circumvent the Directive by transmitting regulated data outside of Europe for processing offshore, the Directive specifically prohibits sending personal data to any country without a "level of [data] protection" considered "adequate" by EU standards.[7]

§ 24:2.2 Social and Legal Context Underlying EU Data Directive

Nefarious uses of secret files under World War II-era fascists and post-War Communists instilled in many Europeans an acute fear of the unfettered abuse of personal information—a fear that lingers to this day. Today's Europeans are still vividly aware of secret denunciations that sent neighbors and relatives to work camps. This is a cultural issue difficult for frontier-spirited Americans to understand: In many parts of Europe, a culture of secrecy permeates society to an extent almost unimaginable in the United States. Indeed, this cultural difference—Europe's protections of confidentiality versus the wide-open US ethic of free speech and "sharing" feelings and information—may be one of the biggest social divides between the two regions.[8]

As computers took over the warehousing of personal data, Europeans' wariness of secret *government* files morphed into skepticism about *corporate* databases. A feeling arose that only a coordinated legislative response could protect citizens from abuses of their personal information. In the post-war decades, Europeans took a series of steps in this direction, with some countries (Germany, France) passing their own comprehensive data laws.[9] By 1980, the Organisation for Economic Cooperation and Development (OECD) was able to issue "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data,"[10] and in 1981 the European Council (not the EU) issued a "Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data."[11] While the aspiration was for a uniform system of data protection laws across Europe, the OECD and the European Council

4. Directive, ch. I, art. 4(1).

5 *Id.*

6. *See infra* section 24:2.5 The EU data directive could reach a love letter or a gossipy chat because:

   - love letters and gossip tend to contain "information" and "identify" some "natural person"—by definition, "personal data" under Art. 2(a)
   - the writing of a letter, or the speaking of gossip, is an "operation . . . such as . . . use, disclosure by transmission, dissemination or otherwise making [personal data] available"—by definition, "processing of personal data" under Art. 2(b)
   - a letter-writer or gossip is a "natural . . . person"—by definition, a "controller" or "processor" of personal data under Directive Art. 2(d), (e)

While presumably European data agencies do not police love letters and gossip, in fact the European data agencies do actively regulate *business-context* phone calls about fellow workers. *See, e.g., Document d'orientation adopté par la Comision le 10 novembre 2005 pour la mise en oeuvre de dispositifs d'alerte profesionelle* (French CNIL data agency guidelines of 11/05 on whistleblower hotlines). Some EU member states may have implemented an exception (such as under art. 9) that would except certain love letters or gossip, but even so, the data law would reach, and then possibly except, the love letter or gossip. *But cf. infra* note 37 and accompanying text.

7 *See* section 24:3 *infra* (Transfer of Data to Third Countries).

8 *See generally* Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the US and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 441 (2002); Steven R. Salbu, *The European Union Data Privacy Directive and Internal Relations*, 35 VAND. J. TRANSNAT'L L. 655, 668 (2002). However, the cultural aversion to denunciations is much stranger in certain parts of Europe (France and Germany, for example) than in others (such as England and Spain).

9 *See, e.g.,* Huie, Laribee & Hogan, *supra* note 8, at 441–44.

10. OECD Council, Sept. 23, 1980.

11. Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, European Treaty Series, No. 108; *see also* Salbu, *supra* note 8, at 668.

conventions were not self-executing, and data protections across Europe continued to vary widely.

Meanwhile, by the 1980s, a reinvigorated European Union was charging ahead, proactively "harmonizing" (aligning) laws across a wide range of sectors as part of its "Single Market Program"—the initiative that solidified a collection of European countries into a single economic entity, the EU. Simultaneously, new technologies were emerging and threatening personal privacy (personal computers, bar code scanning, closed-circuit video monitoring, the Internet, and, more recently, cellular telephones with digital photography).[12]

These factors created a consensus that, in Europe, regulation should safeguard citizens' personal data from prying governments and corporations. The solution was obvious: Piggyback on EU integration to align Europe's then-inconsistent "data protection" (privacy) laws via a single, pan-European data protection directive.[13]

§ 24:2.3 Definitions

The EU data Directive creates its own jargon, which is essential to master before discussing any EU privacy law issue.

"Personal data" means information about any "identified or identifiable natural person," who is known as the "data subject."[14] "Identified or identifiable natural person" means anyone who "can be identified, directly or indirectly, in particular by reference to an identification number or by one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity."[15]

Accordingly, in the business context, a photo of someone on an identification badge or on a video monitor is "personal data," as is a listing of employee salaries designated either by employee name or some identification number (company ID number, social security number, tax ID number). However, a truly "anonymized" list of data—such as, for example, a list of employee compensation rates at a worksite *not* designated by name or number—would not be "personal data."[16] Thus, genuinely "anonymizing" personal data is always a way to sidestep the application of the Directive.

"Processing of personal data" means "any operation or set of operations . . . performed upon personal data," automatically or otherwise.[17] This definition is wide open, because it includes "collection, recording, organization, storage . . . retrieval . . . use, disclosure by transmission," and "dissemination." By expressly including "storage" in the definition of "processing," the mere *act of holding personal data* is, under EU law, a regulated activity.

Other essential EU Directive jargon:

- A data "controller" is anyone who determines the "purposes and means of processing of the personal data."[18]
- A data "processor" is anyone who processes personal data for a controller.[19]
- A "third party" is anyone who processes data under "the direct authority" of a controller or processor.[20]

§ 24:2.4 Processing Data Domestically in Europe

With these broad definitions as a springboard, the Directive extensively regulates processing of personal data. The Directive's main objectives are:

- To "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of data."[21]

12. *See, e.g.*, Salbu, supra note 8; University of Minnesota, *Directing Digital Dataflows: The EU Privacy Directive and American Communication Practices, available at* www.isc.umn.edu/research/papers/EUdatadirective.pdf. For more on the gulf between US and European attitudes to privacy, *see, e.g., Privacy Rights: EU Has Strict Curbs on Employee Monitoring Compared to Weak Rules in the United States*, Daily Lab. Rep. (BNA) no. 49, Mar. 14, 2006, at A-4.
13. *See, e.g.*, Salbu, *supra* note 8, at 668.
14. Directive, ch. I, art. 2(a).
15. *Id.*
16. *Cf.* Salbu, *supra* note 8, at 670.
17. Directive, ch. I, art. 2(b).
18. *Id.* ch. I, art. 2(d).
19. *Id. See also* ch. II, arts. 10–11. Data subjects are also required to be told of their identities, why the data was collected, as well as the identities of those who receive the data.
20. *Id.* ch. I, art. 2(d).
21. Directive, *supra* note 1, at 38.

- To protect EU citizens from—according to one commentator—the "aggressive wave of data collection and distribution similar to that in the United States."[22]
- To harmonize privacy laws across member state borders, ensuring the free flow of personal data among the EU member states.[23]

The rules the Directive imposes domestically within Europe to achieve these broad objectives break down into three categories:

- Complying with data quality principles and rules;
- Disclosing to data subjects and addressing their concerns;
- Reporting to state agencies.

[A] Complying with Data Quality Principles and Rules

In vivid contrast to the US marketplace of ideas where citizens are free to research and discuss whatever they want, the EU Directive, as worded, actually prohibits all personal data "processing"—except for processing that is done "fairly" and "lawfully" and for "legitimate" purposes.[24] Specifically, the Directive imposes a presumption against "collect[ing]" and "process[ing]" personal data *unless* done "fairly and lawfully," and for "specified, explicit *and* legitimate purposes."[25]

In practice, this means data controllers must process personal data consistent with a number of "data quality principles":

1. *Fairness*. Process data "fairly and lawfully."
2. *Specific purpose*. Ensure that data are processed and stored "for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes."
3. *Restricted*. Ensure that data are "adequate and relevant, and not excessive in relation to" the purposes they are for which they are collected.
4. *Accurate*. Ensure that data are "accurate and, where necessary, kept up-to-date," so that "every reasonable step [is] taken to ensure" errors are "erased or rectified."
5. *Destroyed when obsolete*. Maintain personal data "no longer than necessary" for the purposes for which the data were collected and processed.[26]

In addition to these five listed principles, the Directive elsewhere adds two more:

6. *Security*. Data must be processed with adequate "security" (a "controller must implement appropriate technical and organizational measures to protect personal data against . . . destruction or . . . loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. . . ").[27]
7. *Automated processing*. The "decision[s]" from data processing cannot be "based solely on automated processing of data" that "evaluate[s] personal aspects."[28]

Here are some examples of data processing in a business context that likely would violate the above data quality principles, and therefore be illegal under the European laws that implement the Directive:

- A magazine sells its subscriber list to a direct-mail advertiser (violates "fairness" principle).
- A bank combs its own customer files for leads in marketing estate-planning services (violates "specific purpose" principle).

22. "Member states shall neither restrict nor prohibit the free flow of personal data between Member states for reasons connected with the protection afforded under paragraph 1." Directive, art. 1, sec. II. *See also* Salbu, *supra* note 8 at 659 ("the European Union was concerned that data flows within Europe could be hindered if the rules were not standardized across Member states"); Rick S. Lear & Jefferson D. Reynolds, "Your Social Security Number or Your Life: Disclosure of Personal Identification Information By Military Personnel and the Compromise of Privacy and National Security," 21 *B.U. INT'L L.J.* 1, 24 (2003) (discussing Directive's purposes).
23. *See* Lear & Reynolds, *supra* note 22, at 24.
24. Directive, ch. II, art. 6(1)(a), (b).
25. *Id.* (emphasis added).
26. *Id.* ch. II, art. 6(1).
27. *Id.* ch. II, art. 17(1). However, the security "tail" does not wag the data privacy "dog": A common misperception in the US is that if a database is reasonably secure from hacking, it must therefore comply with the EU data Directive. In fact, of course, data security under the Directive is just one principle at work in a much broader law focused chiefly on issues unrelated to security.
28. *Id.* ch. II art. 15(1). Sometimes these principles are articulated a bit differently, but with essentially the same effect. *See, e.g.*, Jörg Rehder & Erika Collins, "The Legal Transfer of Employment-Related Data to Outside the EU: Is It Still Even Possible?", 39 *INT'L L.* 129, 133 (2005).
29. *Id.* ch. II, art. 7(a)–(b).

- A job application for a high-level position asks applicants for information about their primary education and military experience (violates "restricted" principle).
- A credit bureau customer complains about a claimed error in her account—but no one at the credit bureau does anything about it (violates "accurate" principle).
- An employer retains computer backup files, attendance records, and other business information going back many years (violates "destroyed when obsolete" principle).
- An accounting firm's night janitors straighten up piles of client files (violates "security" principle).
- A company's website allows applicants to apply for a job; resumes are screened with a special program that searches for key words (violates "automated processing" principle).

But even complying with these data quality principles is not enough. The Directive goes on to impose a separate hurdle prohibiting some data processing even *consistent* with these principles. Indeed, *all* processing of data—even consistent with the principles—is actively illegal, *unless*:

- the data subject consents, or
- the processing is "necessary" (not merely convenient) to accomplish one of five objectives:
  - "perform[ ] . . . a contract to which the data subject is party";
  - "compl[y]" with a law;
  - "protect" the data subject's "vital interests";
  - advance the "public interest" or facilitate "the exercise of official authority"; or
  - further the controller's (or some other "disclosed" party's) "legitimate interests" without infringing the data subject's "fundamental rights and freedoms."[29]

Therefore, in Europe, processing ordinary personal data is presumed illegal, unless the processing both (1) complies with all seven data quality principles and (2) is either consented to or "necessary."

These are the rules that cover ordinary personal data. Then, on top of this set of rules, the Directive adds a layer of extra rules for a few classes of information now known as "sensitive" data: personal data that discloses "racial or ethnic origin, political opinions, religious and philosophical beliefs, trade-union membership, [or] . . . health or sex life."[30] The Directive flatly prohibits processing all sensitive data[31] unless an express exception applies—including, notably, an "explicit consent," "freely given."[32]

As extensive as the sweep of the Directive is, however, member states have some leeway in carving out certain exceptions, such as for national security, defense, criminal investigations, and the like.[33] The Directive also has member states grant limited exceptions for "journalistic" and "artistic or literary expression,"[34] but only to the extent "necessary" to balance data privacy rights with "the rules governing freedom of expression."[35] And the Directive allows an exception for processing certain "historical, statistical, or scientific" data.[36] Further, some authorities claim that European controllers can freely process data for personal or household use, and that nonprofit organizations may process "sensitive" data about their members.[37]

[B] Disclosure of Processing to Data Subjects

Once someone in Europe is positioned to process personal data consistent with all these principles and rules, the analysis turns to disclosures to data subjects.

The EU data Directive prohibits processing personal data in secret. European data subjects enjoy a legal right to see what information others have on file about them, and to learn what is being done with it.[38] This right can seem revolutionary to US businesses used to

30. *Id.* ch. II, art. 8(1). Data authorities in individual member states, by express rule or otherwise, might add other categories of data not on this list as "sensitive"—for example, age, salary, credit card number.
31. *Id.* ("Member states *shall prohibit* the processing of [sensitive] data") (emphasis added).
32. *Id.* ch. II, art. 8(2)(a); ch. I, art. 2(h). The list of exceptions is *id.* ch. II, art.8(2).
33. *Id.* ch. II, art. 13(1).
34. *Id.* ch. II, art. 9.
35. *Id.*
36. *Id.* ch. I, art. 6(b).
37. *See, e.g., Privacy and Business—The EU Data Privacy Directive, available at* www.privacilla.org/business/eudirective.html. *But cf. supra* note 6.
38. Directive at ch. II, arts. 10, 11; *see* arts. 12, 14.

processing personal information without ever mentioning anything to individuals affected. For example, US grocers quietly track consumer purchases via bar-code scanners. US magazines and baby-photo studios surreptitiously sell customer lists. US employers restrict workers' access to their own personnel files.

In Europe, on the other hand, the EU data Directive requires telling individuals what data are on file about them. The notice must say why the information was collected, who collected it, and who can access it.[39] Additionally, the data subject must have access to the information itself, "without constraint at reasonable intervals and without excessive delay or expense."[40] A data subject who claims some error in his data can offer corrections or ask the controller to purge the incorrect information.[41] A data subject may object "on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties . . . and to be expressly offered the right to object free of charge to such disclosures or uses."[42] If a dispute about the data arises, the Directive sets out complex dispute-resolution mechanisms.[43]

[C] Reporting Data Processing to Data Protection Authorities

The EU data Directive requires each member state to set up its own "Supervisory Authority" or "Data Protection Authority" (DPA)—a bureaucracy or government agency dedicated to privacy— to administer its data protection law.[44] Member states can, and many do, require controllers to file annual summaries of all personal data processing they are doing.[45] The summaries generally need to include the controller's name, the purpose and description of the processing, recipients, and any proposed transfers of data to third countries.[46] Compliance with these local-country disclosure laws can require real attention to detail. In recent years, compliance oriented multinationals based in the United States have been actively driving, from headquarters, initiatives designed to ensure that all their local operations meet these filing requirements.

In practice, different member states handle the disclosure requirement in very different ways. France and the United Kingdom are two states with proactive DPAs that require controllers to file fairly comprehensive annual disclosures. In fact, France's DPA even retains a right affirmatively to *approve* certain proposed data processing operations, which in France are illegal *until* the French Supervisory Authority (known by the French acronym CNIL) issues a specific approval. This CNIL procedure was widely publicized in the summer and fall of 2005, when France denied McDonald's and a unit of CEAC Technologies permission to operate Sarbanes-Oxley whistleblower hotlines, and then issued regulations on this topic.[47] At issue were the data privacy rights of the accused wrongdoer subject to a whistleblower's complaint.

Once a DPA receives required disclosures, it assesses how controllers' processing procedures present specific "risks to the rights and freedoms of the data subjects."[48] The DPA then "publicize[s]" the data processing "operations" it learns about.[49] DPAs also have enforcement powers, and data subjects have private rights of action.[50]

39. *Id.* at ch. II, arts. 10–12, 14. *See* Lear & Reynolds, *supra* note 22, at 24.

40. Directive, ch. II, art. 12(a); *see* Salbu, *supra* note 8, at 672. While datasubject- right-of-access is a critical piece of the Directive, some question whether it is self-activating—an "automatic burden" on data controllers. *See id.* at 672. Member states, undoubtedly, can force data controllers to out notification information automatically. But a lenient interpretation would hold that—absent direct member state compulsion—a data controller need only send required information to those data subjects who expressly request it. *Id.* ("either approach would be in compliance with a strict, literal interpretation of the right to obtain the data").

41. *Id.* ch. II, arts. 12(b), (c); 14.

42. *Id.* ch. II, art. 14(b).

43. *Id.* ch. II, arts. 10, 12, 14; ch. III, arts. 22–24; ch. VI, art. 28. For an analysis of the Directive's dispute resolution procedures, *see* Dowling, *supra* note 3, at 40–43.

44. Directive at ch. VI, art. 28

45. *See id.* ch. II, arts. 18–19; *see infra* section 24:4.

46. Directive at ch. II, art. 19 (1)(a)–(f). Data transfers to third countries are discussed *infra* at section 24:3.

47. CNIL Decision 2005-110, rendered on May 26, 2005, relating to a request for authorization by McDonald's France to put in place a system of professional integrity, Request no. 1065767, *available in unofficial translation at* www.theworldlawgroup.com/newsletter/details.asp?ID=1243487122005; CNIL Decision 2005-111 rendered on May 26, 2005, relating to a request for authorization by the Compagnie européenne d'accumulateurs to put in place ethics hotlines, Request no. 1045938, *available in unofficial translation at* www.theworldlawgroup.com/newsletter/details.asp?ID=1246367122005. As to the CNIL guidelines, issued November 10, 2005, see Document d'orientation, *supra* note 7; as to "frequently asked questions" explaining these guidelines (in French), see FAQ *sur les dispositifs d'alerte professionelle*, 1 Jan. 2006, *available at* www.cnil.fr/index .php?id=1969&news[uid]=324&cHash=7a0521a754. *See generally* EU Commission Article 29 Working Party Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking, and Financial Crime, Doc. 00195/06/EN WP 117 (Feb. 1, 2006).

48. *Id.* ch. II, art. 20(1).

49. *Id.* ch. II, art. 21.

50. *Id.* ch. II, arts. 10, 12, 14, ch. III, arts. 22–24, ch. VI, art. 28.

§ 24:3 Transfers of Personal Data Outside Europe

All the aspects of the EU data Directive we have discussed to this point apply within Europe. We have not yet raised what tends to be the primary EU privacy law compliance challenge confronting US-based multinationals' headquarters: the Directive's provisions on transmitting personal data outside Europe.

As soon as the EU decided to regulate personal data, as a practical matter it had to impose tight limits on transmitting personal information abroad. By imposing the data restrictions we have discussed on European data controllers—data quality principles, disclosures to data subjects, reports to state agencies—the EU faced a huge risk that, rather than comply, certain European data controllers might simply transmit and process European data subjects' personal data somewhere offshore, be it in Nigeria, Haiti, Mexico, Japan, the United States, or any other country without domestic data protection laws like Europe's. Scofflaw European data controllers could elude the Directive entirely, simply by processing European data offshore.

To plug what otherwise would be a gaping hole, the Directive imposes tight limits on transmitting personal data outside of Europe. These limits have profound effects on many US-based multinationals' worldwide operations. And these EU data protection rules attract most attention from multinationals' headquarters outside Europe.[51]

Many a US-based company has been caught off guard to learn that EU data law reaches even internal information about company customers and employees transmitted to US headquarters. A typical US response is that the Europeans are overreaching when they impose their data protection rules on intracompany data housed at US headquarters or on a US-based server. But from a European standpoint, these data transfers, even though intracompany, nevertheless transmit personal data about European data subjects outside Europe's jurisdictional reach. To a European who takes comfort in the EU's tough data protections, transfers of personal data outside Europe, even intracompany transfers, raise a real risk that personal data offshore becomes susceptible to abuse.[52]

§ 24:3.1 Data Transfers to Countries with "Adequate" Data Protection

The Directive dedicates its chapter IV to requirements for sending personal data outside Europe. The core provision here seems sweeping: No data can leave Europe unless the transmission goes to some "third country" that "ensures an adequate level of protection."[53] In other words, data about European individuals can only go into countries with data protection laws that the European Commission considers adequately safeguard Europeans' personal data.

That sets the bar amazingly high: To date, the EU Commission has formally designated only Argentina, Canada, Guernsey, Isle of Man, and Switzerland as "third countries" offering this "adequate level of protection."[54] This formal Commission designation means that transmitting personal information from, say, Romania to Argentina

51. *See* Directive at ch. IV, arts. 25–26.

52. While the fact of the Directive's extraterritorial provisions causes significant compliance problems for US-based multinationals, jurisprudentially these provisions do not stretch the long arm of the law. Contrary to a fairly widespread misunderstanding, the EU Directive does not regulate *overseas* personal data. Rather, it merely imposes restrictions on transmitting *domestic European data* abroad, and it attaches some restrictions onto European information that migrates abroad. The concept is perhaps similar to tax laws that prohibit taxpayers from earning income domestically but paid directly into offshore accounts. The EU data laws, even as applied extraterritorially, do not generally reach anyone other than EU resident data subjects.

53. *Id.* at ch. IV, art. 25(1) (emphasis added). According to the Directive at ch. IV, art. 25(2), the Commission evaluates a jurisdiction's "adequa[cy]" in light of a non-exclusive list of factors:
    - the nature of the data
    - the purpose and duration of the proposed processing operations
    - the country of origin and country of final destination
    - the rules of law in force in the third country (both general and within the data privacy sector)
    - the professional rules and security measures in place in the third country

    The operative standard is indeed "adequac[y]," not *equivalence* to EU data law—but article 25 empowers the Commission unilaterally to deter-mine what is "adequate." *See generally* European Commission Working Document, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98 at 5.54.

54. In addition, the three countries of the European Economic Area (EEA) besides the EU states and Switzerland—Iceland, Norway and Liechtenstein—are also part of this "club," for these purposes, because in compliance with their EEA obligations, Iceland, Norway and Liechtenstein transposed the EU data Directive. The Commission has said it is unlikely to adopt adequacy findings under Article 25(6) for more than a limited number of countries in the near future. *See* Commission Decision2001/497/EC, 2001 O.J. (L181) at 20; European Union, *Commission decisions on the adequacy of the protection of personal data in third countries, available* at http://europa.eu.int/comm/justice_home/fsj/privacy/ thirdcountries/ index_en.htm.

is legally no different from sending data from Ireland to England. For most legal purposes, this club of countries, together with the European Economic Area (Iceland, Norway, Liechtenstein),[55] forms a sort of "EU data zone."

The problem, of course, is the rest of the world—sending personal data out of Europe to the United States or to any other non-EU/EEA jurisdiction on Earth other than Argentina, Canada, Guernsey, Isle of Man, and Switzerland.[56] Under a strict reading of the Directive's article 25(1), personal data transmissions to any other country would appear flatly illegal, because the text of the Directive's article 25 consistently talks in terms of whether a "third country" offers an "adequate level of protection."[57] This would seem an all-or-nothing proposition of comparative law: Either a "third country" has enacted a generally applicable privacy law that the EU Commission deems "adequate" (therefore making the country eligible to receive personal data from Europe), or it has not (therefore keeping it ineligible).

But in practice this all-or-nothing analysis quickly devolved to mean something very different from what article 25's many references to "third countr[ies]"[58] would seem to imply. After years of futilely trying, in diplomatic discussions, to convince the United States and other "third countries" to pass omnibus, European-style data laws offering "adequate ... protections,"[59] the EU Commission loosened up and began promulgating ways for individual overseas data processors to bind their institutions "adequate[ly]" to EU-style data "protections"—empowering them to receive data from Europe, not country-by-country, but company-by-company.

There are now three such methods, or tools, for a non-European entity to become unto itself its own island nation ("third country") of article 25 "adequate ... protection":

- safe harbor;
- binding/model/standard contractual clauses; or
- binding corporate rules.[60]

Further, the Directive's article 26(1) authorizes a number of *other* exceptions, yet other ways legally to transmit personal data outside of Europe even to a "third country" that fails to offer an "adequate level of protection." A data controller or processor can legally send personal data outside of Europe to the United States, or any other country, if:

(a) the data subject has [freely] given his consent unambiguously to the proposed transfer [to be enforceable, a consent must indeed be unambiguous and freely given; EU data authorities take the position that a consent must specifically list the categories of data and the purposes for the processing outside the EU; in the employment context, consents may be deemed presumptively *not* freely given, merely because of the imbalance in bargaining power between employer and employee]; or

(b) the transfer is *necessary* [not merely convenient] for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is *necessary* [not merely convenient] for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is *necessary* [not merely convenient] or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

55. *See supra* note 54.
56. Or other than to Iceland, Norway and Liechtenstein. *See* supra note 54.
57. *See* Directive at ch. IV, arts. 25(1), (2), (3), (4), (6).
58. *Id.*
59. *See, e.g., Struggle Continues with EU Personal Data Protection Directive*, EURO-WATCH, Jan. 15, 1999, at 1.
60. Each of these individualized methods, or tools, is discussed in the immediately following sections.

(e) the transfer is *necessary* [not merely convenient] in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.[61]

Also, of course, there is no prohibition against transmitting genuinely *anonymized* data out of the EU. Where the identity of the data subject is impossible to determine, the data transmission falls outside the scope of the directive.

Therefore, even a business (or other data processor) in a country that is not a member of Europe's club of data-law countries can legally receive information about identifiable individual Europeans (including the business's own customers and employees), but only if(1) the transmission meets one of the narrow article 26(1) exceptions above or (2) the transmission is sheltered under one of the three individualized methods for transferring data discussed below: safe harbor, binding/model/standard contractual clauses, and binding corporate rules.

§ 24:3.2 Safe Harbor

Because Europe sees the United States as a "third country" that fails to offer an "adequate level of [data] protection,"[62] the EU data Directive looms as a huge barrier for US-based multinationals' headquarters that need data on their own European customers, suppliers, and employees. As soon as the Directive became effective in1998, it became clear that it actively threatened data flows between the two largest trading partners on Earth—such as, for example, most Europe-to-United States data flows involving the following:

- interactive websites and company intranets;
- customer reservations, frequent-customer databases, customer help lines, and other trans-Atlantic customer service operations;
- customer and employee directories;
- routine financial transactions including ATM, credit card transactions, and check-clearing;
- administration of equity plans, expatriate programs, succession management, and other trans-Atlantic human resources functions;
- human resources information systems (PeopleSoft, SAP, Oracle, Ceridian, and the like); and
- routine mail, express delivery documents, e-mails, and telephone calls.

Not surprisingly, maintaining EU-to-US data flows under the Directive materialized as a key business issue on even the *diplomatic* radar screen. In the late 1990s, the EU Commission and the US government, led by the Department of Commerce, launched formal discussions to come up with a solution tailored for US businesses.[63] Initially the EU Commission—perhaps naively—hoped to convert the Americans: Brussels diplomats spent almost a year trying to convince US officials that a comprehensive data law modeled on the Directive would protect Americans and strengthen US interests.[64] However, the immense cultural and free speech divide[65] kept the United States from seriously entertaining membership in Europe's club of "third countries" offering "adequate level[s] of protection."[66]

So the European Commission and the US Department of Commerce turned to tailoring a bespoke US solution that became "safe harbor."[67] As soon as the Europeans and Americans hammered out this safe harbor compromise, the EU Commission ratified it via a special "decision."[68] (A decision is a form of EU legislation that, unlike a directive, applies directly across Europe without member state ratification.)

61. *Id.* ch. IV, art. 26(1) (emphasis added).
62. *See supra* notes 56–60 and accompanying text.
63. *See, e.g.,* "Struggle Continues with EU Personal Data Protection Directive," *supra* note 59.
64. *Id.*
65. *See supra* sections 24:1, 24:2.2.
66. *See supra* section 24:3.1.
67. *See, e.g.,* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 396 (2003).
68. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council of the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, 2000 O.J. (L215) 7 [hereinafter "Safe Harbor Decision"]. In tandem with the EU Safe Harbor Decision, the US Department of Commerce issued Frequently Asked Questions on 21 July 2000 [hereinafter "FAQ"] offering guidance.

Safe harbor, which is unique to the United States because it is completely unavailable elsewhere, is a voluntary self-certification system for transmitting data from the EU to the United States—but not beyond. Under it, US data processors can receive personal data from Europe if they agree to accept restrictions requiring them to treat the data as if still physically in Europe and subject to the Directive. In Directive article 26 terms, a safe harbor entity essentially becomes an autonomous "third country" free to receive personal data from Europe as a full-fledged member of the club of "countr[ies]" offering "an adequate level of protection."[69] (Contrary to a widespread misconception, safe harbor restrictions need apply only to personal data *about European data subjects*: A safe harbor company remains free to deny EU-style data protections to, say, American data subjects.)

Because the safe harbor structure wraps personal data from Europe in a blanket of EU data Directive compliance, the substantive safe harbor requirements essentially track the Directive's data quality principles and rules.[70] Thus, self-certifying under safe harbor requires publicly committing, on the US side, to comply with seven safe harbor principles.[71] In addition, self-certifiers have to:

- disclose their privacy policies publicly;
- accept jurisdiction of the US Federal Trade Commission (FTC) under section 5 of the Federal Trade Commission Act (which prohibits unfair or deceptive practices affecting commerce), or of the US Department of Transportation under 49 U.S.C. §41712;[72] and
- notify the US Department of Commerce of the self-certification (procedurally, self-certifying merely entails filling out a short form on the Department of Commerce's website, but that form certifies the entity already has in place fully compliant data processing systems and protections).[73]

Organizations qualify for the safe harbor in three ways. The standard route is to develop an in-house privacy policy (covering at least personal data received from Europe) that complies with the safe harbor principles.[74] A less traveled route is to join a self-regulatory privacy program that complies.[75] In addition, an organization subject to a statutory, regulatory, administrative, or other body of law (or rules) that effectively protects personal privacy might also, in theory, qualify.[76]

[A] Seven Safe Harbor Principles

Broadly, we have seen that safe harbor requires US self-certifiers to treat personal data received from Europe as subject to the EU Directive principles we have already addressed.[77] But safe harbor reconfigures these principles and rules a bit, tailoring them to the context of processing EU data inside the United States. Specifically, safe harbor sets out its own seven principles, which track the similar requirements already imposed on domestic EU data processors and controllers. Every safe-harbor-certified company has to follow all

69. *See supra* notes section 24:3.1.
70. *See supra* section 24:2.4[A].
71. *Id.* The public list of safe harbor certified organizations is available at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
72. Under Safe Harbor Decision art. 1 §2(b), self-certifiers submit to a government body in the US empowered to investigate complaints and obtain relief against unfair or deceptive trade practices—a self-certifier that violates safe harbor commits a deceptive trade practice, under US law. Annex VII to the Safe Harbor Decision designates these US government bodies as the FTC and the Department of Transportation.
73. Safe Harbor Decision at 8.
74. *Id.*
75. *Id.*
76. *Id.*
77. *See supra* section 24:2.4.

seven of these principles, or face deceptive trade practices action under section 5 of the FTC Act[78] or another statute.[79]

[A][1] Notice

A self-certifier must ensure that European data subjects are told why a US entity is processing their data.[80] European data subjects must be told the US processor's identity and contact information (for inquiries or complaints).[81] They must be told about their right to limit use, disclosure, and transmission of their data, and how to exercise that right.[82] These communications need to be clear, conspicuous, and communicated as soon as European data subjects are asked to disclose the information that will be sent stateside.[83]

[A][2] Choice

A safe harbor processor must give European data subjects a chance to opt out of having their personal information disclosed to an independent third party (as opposed to an agent) or used for some reason other than why originally collected.[84] This opt-out choice must be clear, conspicuous, readily available, and affordable, and the choice must remain open continuously.[85]

Further, Europeans affirmatively must opt *in* to safe harbor transfers of sensitive information—data about medical and health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sex life.[86] However, exceptions to this opt-in requirement for sensitive data exist, if the processing is

- in the vital interests of the data subject or another person;
- necessary to establish legal claims or defenses;
- required to provide medical care or diagnosis;
- carried out in the course of legitimate activities by a foundation, association or any other non-profit body in pursuit of political, philosophical, religious or trade-union purposes, and under the condition that the data not be disclosed to third parties without consent;
- necessary to carry out an organization's employment law obligations; or
- related to data manifestly made public by the individual.[87]

78. Safe Harbor Decision, *supra* note 68, at Annex II, FAQ 5, at 15. The FTC promised to review, on a priority basis, allegations of safe harbor violations. A range of sanctions can get imposed against a safe harbor company that violates its self-certification: fines; publicity about the violation; an order to delete the non-compliant data; suspension of safe harbor status; an administrative cease and desist order prohibiting the challenged practices; injunctive orders; a complaint in a federal district court. *Id.* at Annex II, FAQ 11, at 22. The FTC will tell the Department of Commerce of whatever action it takes. *Id.*

79. Section 5 of the FTC Act carves out exceptions to FTC unfair/deceptive trade practices jurisdiction; the FTC act simply does not reach: financial institutions; telecommunications companies; interstate-transportation common carriers; air carriers; or meat packers/stockyards. *See* 15 U.S.C. § 45(a)(2). So businesses in these sectors cannot safe-harbor certify, until their governing bodies commit to monitor. *See* Press Release, European Commission, How will the "Safe Harbor" arrangement for personal data transfers to the US work? (Feb. 28, 2002), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/adequacy-faq1_en.htm. Of these governing bodies, so far only the US Department of Transportation has jumped in. The EU Commission now sanctions DOT, along with FTC, in this regard, so airlines can safe-harbor certify. Continental Airlines, for example, has. *See generally* Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (May 28, 2004), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm. The Commission expects other US government enforcement bodies to get Commission authorization later. *See* Press Release, *supra*. Discussions between the Commission and the Department of Commerce with respect to extending the safe harbor to financial services industries were suspended pending implementation of the new Gramm/Leach/Bailey Act. *Id.* For guidance on permissible personal data transfers in the pharmaceutical and medical products industries, see Commission Decision 2000/520/EC at Annex II, FAQ 14, 2000 O.J. (L215) at 23–24.

80. Safe Harbor Decision, *supra* note 68, at 11.

81. *Id.*

82. *Id.*

83. *Id.*

84. *Id.* Under the Onward Transfer Principle, agency relationships may be exempt for this prohibition. *See infra* notes 88–89 and accompanying text.

85. *Id.*, and *id.* Annex II, FAQ 12, at 23.

86. *Id.* Annex I, at 11. *See also supra* note 30 and accompanying text.

87. Safe Harbor Decision, *supra* note 68, at Annex II, FAQ 1, at 13.

[A][3] Onward Transfer

A safe harbor processor wanting to transfer personal data on to some third party agent in the United States or abroad (an "onward transfer") must first verify that the third party agent subscribes to safe harbor principles; is subject to the Directive or another adequacy finding; or signs a "written agreement" binding it to the level of privacy protections under safe harbor.[88] If the third party clears one of these hurdles, the safe harbor party gets a defense, even if the third party ends up violating safe harbor rules—unless the safe harbor party should have known of the problem but failed to take reasonable steps to fix it.[89]

[A][4] Security

Safe harbor processors must take reasonable steps to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.[90]

[A][5] Data Integrity

Personal information on file must be limited to the purposes for which an organization intends to use it. Processed data should be reliable for their intended use, accurate, complete, and current.[91]

[A][6] Access

European data subjects must be offered access to their personal information housed in the United States under safe harbor, and they must have a way to correct, amend, or delete inaccurate information.[92] A safe harbor company can, however, charge a reasonable fee to cover the cost of providing access, and can set reasonable limits on access.[93] Also, a safe harbor company can deny a European data subject access to his own personal data transmitted stateside under safe harbor, as long as one of the following conditions is met:

- the burden or expense of giving access outweighs any risk to individual privacy;
- giving one data subject access would compromise others' privacy rights;
- "proportionality" and reasonableness outweigh privacy interests and justify a restriction;
- disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security, defense, or public security;
- the personal information is processed solely for research and statistical purposes;
- disclosure could interfere with law enforcement (including prevention, investigation or detection of crimes, or the right to a fair trial);
- disclosure could interfere with private causes of action or a fair trial;
- disclosure could breach a legal or professional privilege or obligation;
- disclosure could breach confidentiality of future or ongoing negotiations, such as to acquire a publicly quoted company;
- disclosure could prejudice employee security investigations or grievance proceedings;
- disclosure could prejudice confidentiality necessary for employee succession planning and corporate reorganizations; or
- disclosure could prejudice confidentiality necessary to monitor, inspect, or regulate issues of economic or financial management.[94]

88. *Id.* Annex I, at 11. The "written agreement" is distinct from the model (binding/standard) contractual clauses agreements discussed *infra*. The "onward transfer written agreement" can be much simpler than the model contractual clauses contracts.
89. *Id.*
90. *Id.* Annex I, at 12. *See generally* supra note 27.
91. Safe Harbor Decision, *supra* note 68 at 12.
92. *Id.*
93. *Id.* Annex II, FAQ 8, at 19.
94. *Id.* Annex II, FAQ 8, at 17–18.

The burden to establish one of these exceptions falls on the safe harbor company asserting it.[95]

[A][7] Enforcement

Each European data subject must have ready access to affordable procedures for safeguarding his rights under safe harbor.[96] Therefore, safe harbor companies must build dispute-resolution machinery, and offer it to European data subjects who have grievances.[97] At a minimum, this machinery must include:

- channels for data subjects to post complaints, which the safe harbor company then actually investigates and resolves, awarding damages or other real remedies if there was a violation (these procedures should not be a "show trial"—a widespread perception in Europe sees the chief failing of safe harbor as American data processors too often sweeping European data subjects' complaints under the rug);[98]
- follow-up procedures, conducted either by self-assessment or outside compliance review, verifying that what the safe harbor company claims about its privacy practices is accurate and in place;[99] and
- methods to fix problems, and, for violations, sanctions with teeth.[100]

Two ways a safe harbor company can build this machinery are

- to buy a prepackaged privacy enforcement program that incorporates the safe harbor principles, or
- to submit to legal/regulatory supervisory authorities, such as European data protection authorities (DPAs), that have dispute-resolution machinery already in place.[101]

[B] Safe Harbor's Self-Certification Process

The complexities discussed above can obscure the fact that, procedurally, safe harbor status is amazingly easy to get.[102] All a company need do is log onto the Department of Commerce website and fill out a one-page form, or send a letter self-certifying that it has adequate procedures and protections up and running.[103] Specifically, this self-certification merely needs to disclose:

- the name of organization, mailing address, email address, and telephone and fax numbers;
- a description of how the organization will process personal data received from the EU; and
- a summary of EU personal data handling policy, including:
  - where the privacy policy is available for viewing (if publicly available),
  - effective date,
  - contact office for handling complaints, access requests, etc.,
  - which statutory body has jurisdiction to hear claims for unfair or deceptive practices and other legal violations, FTC or DOT,[104]

95. *Id.*
96. *Id.* Annex II, FAQ 11, at 22.
97. *Id.* Annex I, at 12.
98. *Id.*
99. *Id.* Annex II, FAQ 7, at 16. For detail on how self-assessment works, see *id.* Annex II, FAQ 7, at 16–17.
100. *Id.* Annex I, at 12. On EU data processing dispute resolution procedures generally, albeit not in the safe harbor context, see Dowling, *supra* note 3.
101. *Id.* Annex II, FAQ 5 and 11, at 14, 21. For more on enforcement, see *supra* notes 78–79. A safe harbor company submits to DPA grievance procedures by declaring, in its safe harbor certification, that it:
    - will satisfy the safe harbor dispute resolution requirements by cooperating with the DPA;
    - will indeed cooperate with the DPA in the investigation and resolution of data subjects' safe harbor complaints;
    - will follow whatever "advice" a DPA gives, where the DPA recommends specific action to beef up safe harbor compliance and remedy a problem, including steps to make whole data subjects who complained; and
    - will confirm in writing to the DPA what measures it actually took.
102. Despite the relative procedural simplicity of certifying for safe harbor certification, one survey of US multinationals found that safe harbor is relatively uncommon: 90% of respondents were not certified for safe harbor. David Bender & Larry Ponemon, *Binding Corporate Rules for Cross Border Data Transfer,* 3 RUTGERS J.L. & URBAN POL'Y 154 (2006) (hereinafter "Bender & Ponemon").
103. *See id.* Annex II, FAQ 6, at 15.
104. *See supra* notes 78–79.

- which privacy programs the organization subscribes to,
- what is the organization's method of compliance verification (in-house or third party), and
- what independent body will investigate unresolved complaints.[105]

Then, every year, the organization actively needs to renew its safe harbor status with a short refiling.[106] Original selfcertifications and annual refilings are posted on the Department of Commerce website.[107]

[C] Criticisms of Safe Harbor

From multinationals' point of view, a chief drawback of safe harbor is that it insulates only EU-to-US data transfers, and as such is useless when a conglomerate wants to roll out a globally accessible data base, such as a global human resources information system, or else to transfer data beyond the United States (say, to a back office operation in India). Quite apart from that data-controller-perspective shortcoming, however, are the criticisms of safe harbor as ineffective in safeguarding the rights of EU data subjects.

Because safe harbor emerged as a compromise between the EU Commission and the US Department of Commerce very different from what either party had originally wanted, and because safe harbor is a unique-in-the-world arrangement that applies only to the United States, it should not be surprising that safe harbor has attracted criticisms from the beginning.[108] Detractors tend to focus on shortcomings in compliance: Safe harbor is a self-certification system without mandatory independent verification of what a business actually does. (Safe harbor companies can have an independent body check their compliance up front and annually thereafter, but independent-body checkups are not required, and few companies seem to do them.) The fact that safe-harbor enforcement tends to be complaint-driven, rather than overseen by regulators, and the fact that US enforcement agencies seem rarely if ever to initiate proceedings to enforce safe harbor on the US side, make Europeans nervous—especially in light of Europeans' fear that US data processors are less than vigilant about complaints coming from across the Atlantic.

In October 2004, the EU Commission issued an update on how safe harbor was faring.[109] Besides addressing the compliance issue,[110] the Commission's two other chief concerns were these:

- Some safe-harbor companies never publish a privacy policy; others publish policies that fall short of complying with safe harbor. The absence of a compliant, publicly available privacy policy essentially divests the FTC of jurisdiction, because the FTC cannot prove unfair or deceptive trade practices against a company that never made a false privacy claim in the first place. The Commission document offers several suggestions to the Department of Commerce, asking it to get more engaged and scrutinize organizations that self-certify.[111]
- Up to 30% of safe harbor companies transmit human resources data to the United States, but the Commission is not convinced that the FTC has enforcement power in these situations (could a false statement about internal HR procedures really be a deceptive trade practice?).[112]

§ 24:3.3 Binding/Standard/Model Contractual Clauses

Safe harbor aside, a completely separate way legally to transmit personal data outside of Europe is under so-called "binding," "standard," or "model" contractual clauses. The text of the Directive itself lets the Commission approve transfers of personal data even to third countries that fail to ensure an "adequate level of protection"[113] if the controller erects "sufficient safeguards" via "certain standard contractual clauses" consistent with a "Commission's decision."[114]

105. *Id.*
106. *Id.*
107. *Id.* Annex II, FAQ 6, at 15–16. The website is http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
108. *See, e.g.,* J. Rehder & E. Collins, supra note 28, at 150–51.
109. Commission of the European Communities, Working Document on the Implementation of Commission Decision 520/2000/EC and the Adequacy of the Protection of Personal Data Provided by the Safe Harbor to Date, Commission Staff Working Document, SEC (2004) 1323 (Oct. 2004).
110. *Id.* at 14.
111. *See id.* at 13.
112. *Id.*
113. *See supra* section 24:3.
114. Directive at ch. IV, art. 26(4).

In 2001, 2002, and 2004, the Commission issued three separate decisions[115] anointing three different boilerplate contracts as appropriate cover for an EU data controller ("data exporter") to send personal data to controllers and processors abroad ("data importers").[116] The three decisions effectively created preapproved adhesion form contracts that data importers and exporters can accept or not accept in whole. To negotiate terms within the form contracts would kill the Commission's protection, so after a data exporter and importer decide to use a model contract, all there is to negotiate is which of the three forms to use.[117]

[A] Obligations of the Data Exporter and Data Importer

Speaking very broadly, the Commission's model contracts act like private safe harbor arrangements, where a US data importer contractually pledges to follow a package of rules that fairly closely track the obligations of safe harbor.[118] While details differ among the three model contract forms, in essence a model contract party picks up the burden to process data European-style, with purpose limitation; data quality and proportionality; "transparency"; security and confidentiality; data subject right of access, rectification, and dispute resolution; restriction against onward transfers; special rules for sensitive data; restrictions regarding direct marketing; and automated decision making.[119]

Although the model contractual clauses themselves are pure boilerplate, parties must specify in an appendix the precise categories of data and types of processing involved. Parties must also say whether they will transmit any sensitive data.[120] And parties to model contracts have to promise to respond to reasonable inquiries from data subjects and supervisory authorities,[121] as well as commit to accepting data audits by data exporters or independent inspection bodies.[122]

[B] Apportionment of Liability

If a party breaches a model contract, data subjects—third party beneficiaries—who suffer injury can win compensation from the data exporter or importer, as could a member state data protection authority.[123] Under one of the three model contracts, the data exporter and data importer are jointly and severally liable unless they agreed to indemnify one other.[124]

However, one of the other sets of model clauses[125] lays out an alternate liability regime based on due diligence obligations. This model exposes the data exporter and data importer to liability in proportion to their respective breaches of the contract.[126] Obviously this approach is especially attractive to parties at arm's length (as opposed to parties within a corporate family).[127] To prevent abuses, under this regime member-state data protection authorities get beefed-up powers to cut off data transfers.[128]

115. As mentioned *supra*, a decision is a form of EU legislation that, unlike a directive, applies directly across Europe without member state ratification.

116. Commission Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, 2001 O.J. (L181) 19 (first set of clauses for controller-to-controller transfers); Commission Decision 2002/16/EC on standard contractual clauses for the transfer of personal data to processors established in third countries, 2002 O.J. (L6) 52 (clauses for controller-to-processor transfers); Commission Decision 2004 /915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004 O.J. (L385) 74 (second set of clauses for controller-to-controller transfers).

117. *See id.*

118. *Compare* Decisions, *supra* note 116 *with* Safe Harbor Decision, *supra* note 68.

119. See Decisions, *supra* note 116; *cf.* discussion of these obligations *supra* section 24:2.4[A]; 24:3.3. In other words, a party committing to a model contract will contractually assume burdens similar to the seven principles discussed at 24:3.3 (speaking broadly).

120. *See* Decisions, *supra* note 116. As to sensitive data, see *supra* note 30 and accompanying text.

121. *See* Decisions, *supra* note 116.

122. *See id.*

123. *See id.*

124. Decision 2001/497/EC, *supra* note 116, at 26. As to forum, a data subject can invoke mediation, arbitration, or the courts of the data exporter's home member state. *Id.*

125. Decision 2004/915/EC, *supra* note 116. This set of clauses was initially proposed by a coalition of business associations which sought more business-friendly clauses. *See* Press Release, European Commission, Standard contractual clauses for the transfer of personal data to third countries—Frequently asked questions (July 1, 2005), *available at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&language=EN.

126. Decision 2004/915/EC, *supra* note 116, at 74.

127. Often multinational conglomerates use model contractual clauses intra-company, with European corporate-family entities as data exporters, and US sibling entities as data importers.

128. Commission Decision 2004/915/EC, *supra* note 116, at 75. In addition to the three sets of pre-approved contractual clauses, under the Directive the national data protection authorities have power to authorize one-off (case-by-case) data transfers even to countries not offering "adequate protections," if the data exporter can demonstrate adequate safeguards. Directive at ch. IV, art. 26(2).

§ 24:3.4 Binding Corporate Rules

Safe harbor and model contractual clauses each have serious shortcomings. One huge one: Both regimes envision simple Party-A-to-Party-B data transfers from Europe to a single offshore country. In the real world, though, data transfers are more complex. For example, there are multinational conglomerates that (for example) daily:

- email personal data to recipients in several countries simultaneously;
- input personal data onto globally accessible intranets and human resources information systems;[129]
- zap information back and forth among sister companies and outsource partners; and
- use complex chains of onward transfers, such as from Europe to US headquarters and then to back-office operations in, say, India, and ultimately back to Europe.

Neither safe harbor nor model contracts were engineered to accommodate these multifaceted international data transfers. To customize a more effective tool, in June 2003 the Article 29 Data Protection Working Party—an EU data protection advisory body established under the Directive itself[130]—published a working paper outlining a third way to send data to third countries whose laws fail to offer "adequate protections."[131] So-called "binding corporate rules" (BCRs) are corporate codes of conduct that legally bind each entity of a conglomerate to company-specific, EU-compliant data handling systems. That is, under BCRs, a multinational builds its own in-house structure sheltering the data processing of its branches and partners worldwide. Once approved, BCRs empower the multinational freely to transfer personal data on EU data subjects in-house, worldwide.

BCRs are an intriguing but (as of 2007) still largely untested tool. What is certain is that BCRs are not for the fainthearted or the tight-budgeted. For a large conglomerate to get final BCR approval could cost millions of dollars and take a couple of years. BCRs demand far more thorough global data protection systems, and attract far more intrusive data protection authority (DPA) bureaucratic approvals, than safe harbor or model contractual clauses.[132] BCRs will appeal most to well-capitalized multinationals that genuinely respect privacy rights and commit to top-down EU data law compliance. A conglomerate opting for BCRs is likely to be in the data-processing business (in one way or another); it will have a robust business case justifying this all-bells-and-whistles approach.

How do BCRs work? Our blueprint is yet another working paper from the Article 29 Working Party, issued almost two years after the first one, in April 2005.[133] The 2005 working paper requires a BCR applicant to apply to its most "appropriate" DPA.[134] To get its BCRs approved, the applicant asks the lead DPA to approve its draft BCR package, which spells out exactly how the applicant processes and protects EU personal data worldwide. If, after the inevitable back-and-forth, the lead DPA provisionally approves the package, it then sends it on to every other affected member state DPA. Then the other DPAs can object. Final approval comes when all sign on. The BCR application process will likely be made easier for companies wishing to pursue this method of compliance with the recent publication of a Standard Application for Approval of Binding Corporate Rules, published by the International Chamber of Commerce (the same organization that helped draft the most recent, "business-friendly" model contract).[135] The Standard Application contains eight sections, and is designed to include all information that a DPA would require to make an approval decision on the

129. EU-originating personal data inputted on a computer system run from a server outside Europe are deemed transferred outside the EU. Indeed, even as to servers in Europe, data that are accessed—or accessible—from outside the EU, it is argued, are possibly transmitted offshore.

130. Directive at ch. V, art. 29.

131. Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, EU Article 29 Data Protection Working Party Working Paper 74 (WP 74), June 3, 2003.

132. *See* Bender & Ponemon, *supra* note 102, at 163 ("in practice, for a number of reasons, it may still prove difficult to use BCRs for transfers from more than a single EU member state").

133. WP 108 Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, EU Article 29 Working Party Working Paper 108, Apr. 14, 2005 [hereinafter "WP 108"].

134. WP 108 at §3.5. The DPA to which the conglomerate actually applies can decide whether it in fact *is* the most "appropriate"; if not, it transfers the application to the right DPA. This analysis turns on a host of factors, with location of European headquarters the primary one. *Id.* §§3.3.1, 3.5. Insubmitting a BCR application, a multinational has to include a list of all the member states from which it will transfer personal data. This list tells the lead DPA which other DPAs need to sign off on the BCR application. *Id.* §§4.1.1 to .2.

135. Standard Application for Approval of Binding Corporate Rules, *available at* www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/Standard_Application_for_Approval_of_BCRs.pdf.

company's BCRs. The Standard Application is based upon the above-mentioned BCR Working Party documents, and the Working Party is currently reviewing the Standard Application.

Of course, the BCR application package includes the conglomerate's documents that compose its BCRs—all relevant policies, codes, procedures, notices, contracts, and dispute resolution and other systems.[136] The application has to prove a BCR program actually is up and running, with an auditing feature in place. As with safe harbor and model contractual clauses, BCRs have to specify the types of personal data being transmitted; the methods of (and purposes for) the data processing;[137] data security measures; and a system for how the BCR applicant can amend, and report on, its BCR system.[138] A BCR application must also prove that the applicant's data protection systems really are binding, both "internally" and "externally":[139]

- Showing "internal" BCR compliance requires evidence that the BCRs would bind all the applicant's subsidiaries and affiliates—even its partners and subcontractors. A BCR applicant could establish internal compliance, for example, by offering:
  - a headquarters mandate that all affiliates must comply with the BCRs (assuming the corporate bylaws and applicable member states' laws recognize such a declaration);[140]
  - an example of the multinational's contractual clauses with subcontractors requiring BCR compliance and imposing tough penalties for violations;[141] and
  - proof that employees will follow the BCRs[142] (for example, the BCR application could evidence data protection training and compliance programs, references to BCRs in form employment contracts, and disciplinary rules for employees who violate BCRs).[143]
- Showing "external" BCR compliance requires evidence that "individuals covered by the scope of the binding corporate rules [*i.e.,* EU data subjects] must be able to enforce compliance with the rules both via the data protection authorities and the courts."[144] A BCR applicant has to show it has made its internal dispute resolution procedures, remedies, and compliance mechanisms available to aggrieved data subjects.[145] Every BCR application must guarantee that EU data subjects will enjoy all their rights under the data Directive.[146]

In December 2005, General Electric stepped up as the first multinational to get BCRs provisionally approved by its lead DPA,[147] the U.K. Information Commissioner's Office, which issued that provisional approval pending the other DPAs' positions. By 2006, Daimler Chrysler, Philips Electronics, and Accenture also were publicly discussing BCRs.[148]

§ 24:4 "Transposition" of the EU Directive in Selected European States

In the United States we are tempted to think of European data law as a federalized structure emanating from Brussels. In fact, of course, the EU is not a federal system. While each member state's data law incorporates (that is, adopts or "transposes") the EU data Directive, each country's law is unique. Consistent with the advisory

136. WP 108 at §4.1.3. The Article 29 Working Party cautions that a BCR applicant should mark as "confidential" any confidential submission. But as the approving DPA will circulate the whole package to every other interested DPA—some of which are subject to EU member state freedom of information laws—ironically, a confidential BCR data privacy application may end up disclosed to the public. *Id.* §4.1.4. Therefore, "best practice" is to limit a BCR application (to the extent possible) to what is directly relevant to determining the adequacy of draft BCRs. *Id.* §6.3.
137. *Id.* §7.
138. *Id.* §§8–9.
139. *Id.* §5.1.1 to .2.
140. *Id.* §§5.6 to 5.7.
141. *Id.* §5.11.
142. *Id.* §5.9.
143. *Id.*
144. *Id.* §5.13.
145. *Id.* §5.15.
146. *Id.* §5.20.
147. UK Information Commissioner Press Release dated Dec. 22, 2005, "Information Commissioner Authorises General Electric to Transfer Information Overseas," *available* at www.ico.gov.uk/cms/DocumentUploads/binding_corporate_rules.pdf.
148. *Cf.* Privacy Laws & Business International Privacy Officers' Network Conference, "Negotiating Successful Binding Corporate Rules Programs for International Transfers of Personal Data," Washington, D.C., Mar. 8, 2006.

nature of an EU directive (and with the EU principle of "subsidiarity"—home state rule), the member state data laws vary widely.[149]

Having examined how the EU data Directive works as an overall framework, we can now summarize the actual data laws that apply in the European states. While those local laws offer data subjects at least the Directive's core protections, some add extra rights. And all member states have created their own unique DPAs, compliance structures, notification processes, and other bureaucratic procedures. In short, questions about how to comply with data laws in Europe usually end up at the member state, as opposed to EU, level.

The summaries below are broad overviews of some member states' data laws, focusing on the ever-important affirmative duty to register data protection systems with the local DPA.

§ 24:4.1 Denmark

Denmark's Act on Processing of Personal Data, in effect since 2000,[150] is enforced by the Danish Data Protection Agency.[151] Private data processors in Denmark must notify this bureaucracy before they start up any data processing (but there is a handful of exceptions). Danish processors have to disclose:

- their name and address, and those of any representative or other data controller or processor;
- the categories and purposes of the processing;
- a general description of the processing;
- the categories of data subjects, and the categories of data being processed about them;
- whom the data will be disclosed to;
- proposed offshore personal data transfers—plus a summary of the steps that will ensure secure processing;
- launch date for the processing; and
- destruction date for the data.[152]

§ 24:4.2 England

To implement the Directive, the English Parliament passed the Data Protection Act in July 1998, effective March 1, 2000.[153] The Information Commissioner, also known as the Data Protection Commissioner, oversees enforcement.[154] This law (with some exceptions) requires that nongovernmental data processors notify the Information Commissioner's office before processing information, and the information commissioner has indeed been fining nonfilers. While notice-filing costs only £35 per year,[155] the notice requirement means that even routine hiring, filing, customer sales, and e-mailing are illegal in England—until a data notice is on file. That notice must offer:

- the data controller's name and address;
- the name and address of any company-appointed data-law "representative";

149. *See supra* section 24:2 *et seq.* For overviews of the EU system and "subsidiarity," *see, e.g.*, Donald C. Dowling, Jr., *From the Social Charter to the Social Action Program 1995–1997, European Union Employment Law Comes Alive*, 27 CORNELL INT'L L.J. 43, 46–56 (1996); Donald C. Dowling, Jr., *EC Employment Law After Maastrict: Continental Social Europe?*, 27 INT'L LAW. 1, 7–12 (1993); Donald C. Dowling, Jr., *Worker Rights in the Post-1992 European Communities: What Social Europe Means to US–Based Multinational Employers*, 11 NW. J. OF INT'L L & BUS. 564, 574–80 (1991).

150. Act in effect since July 1, 2000; *see* Privacy International's *Privacy Reports, available* at www.privacyinternational.org (follow "PI Reports "hyperlink to hyperlinks alphabetized by country) [hereinafter "*Privacy Reports*"].

151. Act on Processing of Personal Data, Act No. 429 (May 31, 2000) (Denmark), Title VI, Part 16, *available* at www.datatilsynet.dk/eng/index.html.

152. *Id.* Title V, Part 12 §16.

153. *See Privacy Reports, United Kingdom of Great Britain and Northern Ireland*, www.privacyinternational.org.

154. Information Commissioner's Office, www.informationcommissioner.gov.uk/eventual.aspx?id=34.

155. Data Protection Fact Sheet, *available* at www.informationcommissioner.gov.uk/eventual.aspx?id=34.

- a description of personal data to be processed, plus categories of data subject affected;
- an explanation of why data will be processed;
- an identification of who will receive the data; and
- a listing of the non-EU/EEA jurisdictions where the data controller will transfer data directly or indirectly.[156]

§ 24:4.3 France

While it had a broad data protection law that long predated the EU Directive, France took its time tweaking that law to bring it into compliance with the Directive. Missing the October 1998 deadline, France failed to pass its French Data Protection Act, which amended the old law, until July 20, 2004.[157]

French data law is administered by the *Commission nationale del'informatique et des libertés* (CNIL),[158] a proactive agency that enforces the data law vigorously, and which has issued detailed regulations on certain aspects of personal data processing. In France, to process personal data legally, a data controller must:

- notify the CNIL of data files opened, and what they contain;
- tell data subjects their rights;
- ensure personal data are secure, confidential, and kept from unauthorized third parties;
- cooperate with CNIL data audits and requests for information;[159] and
- in certain cases, such as operating certain whistle blower hotlines, obtain affirmative CNIL permission *before* processing any data.[160]

§ 24:4.4 Germany

Like France's original law, Germany's original data protection law long predated the Directive—and, in fact, was a chief inspiration for it. Like France, Germany took its time conforming its data law to the Directive: the Federal Data Protection Act (*Bundesdaten-schutzgesetz*, or BDSG), which is enforced by the German Federal Data Protection Commissioner,[161] underwent a final revision to bring it fully into synch with the Directive only in 2002, thus missing the 1998 EU deadline by about four years.[162]

Under Germany's data law, only a small group of businesses need register descriptions of their data processing systems with the data bureaucracies of the German states (*Länder*). These include businesses that regularly transfer personal data—even if anonymous—to third parties, such as German credit recording agencies, direct marketing companies, and market research institutes. German businesses can exempt themselves from registering requirements if they appoint an internal data protection officer;[163] if they employ fewer than four data processors who process personal data only for in-house purposes; or if their processing is done through data subject consents or contracts with the data subjects.[164] Those businesses that *do* register have to disclose:

- company name and address;
- who represents the company for data purposes;
- why the company processes personal data;
- who the data subjects are, and what data about them the company processes;
- who receives the data;
- rules on deleting data;

156. Data Protection Act, ch. 29, Part III §16 (UK), *available at* www.opsi.gov.uk/acts/acts1998/80029–c.htm#16.
157. *See Privacy Reports, Republic of France*, www.privacyinternational.org.
158. www.cnil.fr/index.php?id=4.
159. www.cnil.fr/index.php?id=41.
160. *See supra* note 47 and accompanying text.
161. *See* German Federal Commissioner for Data Protection and Freedom of Information, *available at* www.bfd.bund.de.
162. *See Privacy Reports, Federal Republic of Germany*, www.privacyinternational.org.
163. Registered under Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBl. I. S. 66, §§ 4f, 4g (F.R.G.) (hereinafter BDSG).
164. BDSG §4d; *see* German Federal Data Protection Commissioner, *Frequently Asked Questions*, www.bfd.bund.de/information/faq_en_comp.html.

- any envisioned transfers to third countries; and
- security measures.[165]

§ 24:4.5 Italy

In 2003 Italy's legislature passed a new "Privacy Code relating to the protection of personal data."[167] The bureaucracy charged with enforcing this law is Italy's Supervisory Authority for Personal Data Protection (*Garante per la Protezione dei Dati Personali*). Italy's data code does not require data processors to notify the *Garante* about their processing unless their systems process "high-risk" data. Under Italian law, "high risk" has nothing to do with "sensitive" data under the Directive;[168] rather, "high-risk" data means data like:

- genetic and biometric information;
- data processed to analyze or profile people; and
- credit-related information.[169]

The *Garante* determines how processors make these disclosures.[170]

§ 24:4.6 Netherlands

The Netherlands was another data protection law straggler. Under the Directive, they were to pass a comprehensive data law by October 1998, but the Dutch missed their deadline by several years; in 2000, they passed their Personal Data Protection Act, a law not effective until September 2001. Until 2001, Dutch business lagged conspicuously behind their European peers in offering data subjects Directive-mandated rights.

A Dutch data protection bureaucracy, the *College Bescherming Persoonsgegevens* (CBP), oversees data law compliance.[171] Subject to a few exceptions, Dutch data processors must affirmatively disclose to the CBP:

- their name and address;
- the purpose of the data processing;
- the types of data subjects;
- who will receive the personal data;
- what data they will transmit offshore; and
- their data security measures.[172]

§ 24:4.7 Switzerland

Switzerland, while not an EU or even an EEA country, is officially an "adequate protections" jurisdiction with an EU-like data law.[173] The amended Swiss Federal Data Protection Act of 1992 (*Loi fédérale sur la protection des données*) regulates personal information that the federal government and private bodies process. A Swiss Federal Data Protection Commissioner enforces the Act. Processors must register their data with this bureaucracy—but only if they regularly process sensitive data or "data profiles," or if they regularly transmit data to third parties, and if:

- this processing is done voluntarily (not pursuant to some le-gal mandate), and
- the data subjects do not know about this processing.[174]

The Swiss Data Commissioner determines how to make these disclosures.

§ 24:5 Data Privacy Laws Beyond Europe

The EU's data protection regime is the world's most comprehensive—and pervasive. But a handful of countries outside Europe also regulate data protection comprehensively, and still other

165. *Id.*
166. [Reserved.]
167. Personal Data Protection Code, Legislative Decree No. 196 of 30 June 2003 (Italy); *see Privacy Reports, Italian Republic*, www.privacyinternational.org.
168. *See supra* note 30 and accompanying text.
169. *See* section 37 of the Italian data code, *supra* note 167, for additional details.
170. *See* the Garante website, www.garanteprivacy.it/garante/navig/jsp/index.jsp.
171. *See Privacy Reports, Kingdom of the Netherlands*, www.privacyinternational.org.
172. Guidelines for Personal Processing, *available* at www.dutchdpa.nl/.
173. *See supra* notes 53–57 and accompanying text. In 2000, the EU Commission anointed Swiss law as ensuring an adequate level of data protection under the Directive. *See Privacy Reports, available at* www.privacyinternational.org.
174. Loi fédérale sur la protection des donées [LPD] [Federal Data Protection Act] June 19, 1992, art. 19 (Switz.), *available at* www.edsb.ch/e/gesetz/schweiz/act.htm.

nations regulate specific aspects of privacy. Indeed, on occasion a nonEuropean country will clone EU data laws in a straightforward bid to attract the Commission's "adequate protections" designation,[175] thereby boosting trade with Europe. Other times, a country with no history of protecting citizens' private data will take baby steps to address data privacy concerns, such as passing rudimentary data laws or enacting a generalized constitutional privacy right.

There are transnational data regimes that loosely parallel the multi-jurisdictional EU approach, but none of these is nearly as comprehensive, robust, or important as the EU Directive. One example is the Asia-Pacific Economic Conference (APEC) Privacy Framework, which suggests to APEC member countries (as diverse as Chile and Singapore) that they adopt data privacy laws, but without specifically spelling out what those laws should be.[176] Unlike the EU Directive, which requires the EU member states to enact ("transpose") comprehensive data protection laws, the APEC Privacy Framework is best described as aspirational: It sets out nine data privacy principles, but it does not mandate that countries adopt them. (The APEC principles may nonetheless be useful to countries with little or no history of data protection.) The APEC Privacy Framework is quite self-consciously a floor and not a ceiling, with a stated purpose to "promot[e] a flexible approach to information privacy protection for APEC Member Economies, while avoiding the creation of unnecessary barriers to information flows."[177] Whether the APEC Privacy Framework will spur any of APEC members to adopt data protection laws (in keeping with the nine enumerated privacy principles, or otherwise) remains to be seen.

The following is an overview of data privacy laws in select countries outside Europe, including some APEC countries.

§ 24:5.1 Argentina

The Argentine constitution, like many others in South America, purports to ensure a right of privacy: Article 43 guarantees a right of so-called "habeas data."[178] Under this principle, anyone can file a lawsuit "to obtain information on the data about himself and their purpose, registered in public records ... or in private ones."[179] In 2000, Argentina supercharged this constitutional right when it codified its Personal Data Protection Act.[180] This law openly tracks the EU Directive,[181] and as we have seen, the EU Commission quickly anointed Argentina's law as offering European-style "adequate protections."[182] Now, personal data go back and forth between Europe and Argentina as freely as within Europe. In substance, Argentina's Act does the following:

- offers general data protection provisions;
- sets out rights and duties of data subjects and controllers;
- launches a supervisory bureaucracy, the Argentine National Directorate for the Protection of Personal Data;[183] and
- fleshes out further procedures on "habeas data."

Argentina's law, consistent with EU rules, also prohibits transferring personal data offshore to countries without adequate protections, such as the United States.[184] Although there is a widespread perception that Argentina is a less-vigilant enforcer of its data rules than are the EU jurisdictions, Argentina has passed a number of laws supplementing its comprehensive data statute:

175. *See supra* section 24:3.1.

176. APEC Privacy Framework Fact Sheet, *available at* www.apec.org/apec/news_media/fact_sheets/apec_privacy_framework.html.

177. *Id.*

178. CONST. ARG., *available at* www.biblioteca.jus.gov.ar/Argentina-Constitution.pdf.

179. *Id.*

180. Personal Data Protection Act No. 25,326 (Oct. 4, 2000) (Arg.), *available at* www.privacyinternational.org/countries/argentina/argentine-dpa.html.

181. *See supra* section 24:2.

182. Because of the Argentine Act's sweep, after a 2002 opinion on Argentina's Data Protection laws from the EU Data Protection Working Party, the EU Commission issued a decision of June 2003 declaring Argentina a third country providing "adequate [data] protections." Opinion 4/2002 on the level of protection of personal data in Argentina—WP 63 of 3 October 2002, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm; Commission Decision of 30/06/2003 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequate protection of personal data in Argentina, *available* at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf.

183. Direccion Nacional de Proteccion de Datos Personales, *available* at www.jus.gov.ar/dnpdpnew/.

184. *See supra* section 24:3.

- A decree from 2001[185] lays out regulations under the act.
- A "disposition" from 2003[186] outlines privacy sanctions and classifies degrees of infractions.
- A "disposition" from 2004[187] enacts a data code of ethics and defines terms for bankers and commerce.

§ 24:5.2 Australia

Australia jumped into the data-privacy-regulation business as early as 1988, when it passed its Privacy Act[188] spelling out eleven "Information Privacy Principles" (IPPs)[189] on the collection, solicitation, storage, security, access, and uses of personal data, but only in Australia's public sector—its six states. Meant to meet obligations under a pair of treaties that Australia had signed onto, this bare-bones law steered clear of many core privacy issues. Later Australia filled in some gaps, passing the following laws:

- Data Matching Program (Assistance and Tax) Act (1990)[190]
- Credit Reporting Code of Conduct (1991)[191]
- Telecommunications Act (1997)[192]
- Spam Act (2003)[193]
- Market and Social Research Privacy Code (2003)[194]
- Privacy Amendment Act (2004)[195] (extending privacy protections to non-Australian citizens).

Nevertheless, until a sweeping amendment of 2000, Australia confined its omnibus privacy law to its public sector. But then the Privacy Amendment (Private Sector) Act of 2000 imposed on private businesses ten new "National Privacy Principles" (NPPs); reaffirmed the eleven principles from the original 1988 law; and addressed, for the private sector, the use, disclosure, and management of personal data—as well as anonymity and offshore data transmissions.[196] The 2000 law

- sets up a "co-regulatory" scheme, letting businesses roll out self-developed "Codes of Practice" that tailor privacy law principles to their operations;
- defines data quality;
- describes how to anonymize data;
- offers an "opt-out" policy for data subjects; and
- exempts "small businesses" (but the Australian government has estimated this exemption reaches 94% of all businesses in Australia).[197]

185. Decree No. 1558/2001 (Mar. 12, 2001), Reglamentación de la Ley No.25.326 (Spanish-language version), *available* at www.protecciondedatos.com.ar/dec1558.htm.
186. Disposition No. 1/2003, Apruébanse la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante las faltas que se comprueben, *available* at www.protecciondedatos.com.ar/disp12003.htm.
187. Disposition No. 4/2004, Homológase el Codigo de Etica de la Asociacionde Marketing Directo e Interactivo de Argentina (AMDIA), *available at* www.protecciondedatos.com.ar/disp42004.htm.
188. Privacy Act 1988, Act No. 119 of 1988 (Austl.), *available at* www.privacy.gov.au/act/privacyact/index.html.
189. Information Privacy Principles, *available at* www.privacy.gov.au/act/ipps/index.html.
190. Data Matching Program (Assistance and Tax) Act, 1990 (Austl.), *available at* www.austlii.edu.au/au/legis/cth/consol_act/dpata1990349/.
191. Credit Reporting Code of Conduct, 1991 (Austl.), *available at* www.privacy.gov.au/publications/p6_4_31.pdf.
192. Telecommunications Act, 1997 (Austl.), *available at* www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.
193. Spam Act 2003, Act. No. 129 of 2003 (Austl.), *available at* www.com-law.gov.au/ComLaw/Legislation/ActCompilation1.nsf/all/search/E9920A4E670D0FC8CA25702600124DC5.
194. Media Release, Office of the Privacy Commissioner (Austl.), Privacy Commissioner approves market research code (Aug. 27, 2003), *available at* www.privacy.gov.au/news/media/03_11_print.html.
195. Privacy Amendment Act 2004, No. 49, 2004, *available at* www.comlaw.gov.au/comlaw/Legislation/Act1.nsf/0/1E1967107CFB7FBECA256F7200112C2E/$file/0492004.pdf.
196. National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000), *available at* www.privacy.gov.au/publications/npps01.html.
197. *Id.*

Australia's regulation on transmitting data offshore[198] is relatively lenient. Australians can legally send personal data abroad, as long as they

- believe the recipient will uphold the Australian law principles, or
- the data subject consents (unless consent is impractical to get), or
- the transfer is necessary to comply with some contract between the recipient and the data subject, or some contract between the recipient and the sender that benefits the data subject.[199]

By US standards, Australia's data regime looks comprehensive. But its Achilles' heels—anemic provisions on transmitting data off-shore and broad exceptions, such as for small businesses and also for employment data—explain why the EU Commission has not seen fit to anoint Australia as an "adequate protections" jurisdiction.

§ 24:5.3 Brazil

Brazil has no comprehensive data privacy law. But it does have on the books some principles that, taken together, add up to a viable system of privacy protection. Like other South American countries, Brazil's constitutional privacy rights look great on paper: The constitution calls the right of privacy "inviolable" and guarantees money to everyone who suffers "property or moral damages resulting from [a] violation."[200] The constitution goes on to guarantee the common South American right of "habeas data." Although more watered-down than Argentina's "habeas data" right,[201] Brazil gives data subjects a right to see data on file about them in government databases, plus channels to correct them.[202]

However, Brazil has no data privacy bureaucracy, nor does it restrict offshore data transmissions. Not surprisingly, therefore, the EU does not recognize Brazil as an "adequate protections" jurisdic-tion.[203] But Brazil's data regulation goes well beyond its constitution, and includes some tough sectoral laws:

- The Consumer Protection Law[204] (1990) protects consumer data in databases and files and lays out procedures for record keeping, plus guidelines for informing data subjects.
- Federal Law No. 8069[205] (1990) regulates personal data of minors.
- Federal Law No. 9296[206] (1996) regulates wiretapping.
- Telecommunications Act[207] (1997) lays out privacy rights in the telecom sector.
- Federal Law No. 9507[208] (1997) clarifies habeas data.
- Financial Institution Secrecy Law[209] (2001) addresses financial data.
- Civil Code[210] (2003) outlines some additional privacy rights.

198. *Id.* Principle 9.
199. *Id.*
200. C.F. art. 5 (Brazil) (Constituição Federal), with reforms through 1998 (hereinafter BRAZ. CONST.), *available at* www.georgetown.edu/pdba/Constitutions/Brazil/brtitle1.html).
201. *See supra* section 24:5.2.
202. BRAZ. CONST. tit. II, ch. I, art. 5, LXXII.
203. *See supra* section 24:3.1.
204. Law No. 8.078 as of Sept. 11, 1990 (Brazil), Consumer Defense Code Provides for Consumers' Protection and Makes Other Arrangements, *available at* www.procon.sc.gov.br/legislacao_04.htm.
205. Lei No. 8.069, de 13 de Julho de 1990, D.O.U. 16.7.1990 (Brazil), *available at* www.planalto.gov.br/ccivil_03/Leis/L8069.htm.
206. Lei No. 9.296, de 24 de Julho de 1996, D.O.U. de 25.7.1996 (Brazil), *available at* www.planalto.gov.br/ccivil_03/Leis/L9296.htm.
207. Lei No. 9.472, de 16 de Julho de 1997, D.O.U. de 17.7.1997 (Brazil), *available at* www.planalto.gov.br/ccivil_03/Leis/L9472.htm.
208. Lei No. 9.507, de 12 de Novembro de 1997, D.O.U. de 13.11.1997(Brazil), *available at* www.planalto.gov.br/ccivil_03/Leis/L9507.htm.
209. Lei Complementar No. 105, de 10 de Janeiro de 2001, D.O.U de11.1.2001 (Brazil), *available at* https://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm.
210. Lei No. 10.406, de 10 de Janiero de 2002, D.O.U. de 11.1.2002 (Brazil), *available at* http://www81.dataprev.gov.br/sislex/paginas/11/2002/10406.htm.
211. *See* Privacy International, *Federative Republic of Brazil* (Nov. 16, 2004),*available at* www.privacyinternational.org/article.shtml?cmd[347]=x-347-83515.

In addition, Brazil's legislature has considered other data protection bills, a number of which are still pending; they would regulate, for example, Internet service providers, criminal records, email spam, Internet privacy, and offshore data transfers.[211]

§ 24:5.4 Canada

Canada enacted a comprehensive federal data protection law, the Personal Information Protection and Electronic Documents Act (PIPEDA),[212] which has come into force in stages since January 1, 2001. PIPEDA regulates the collection, use, and disclosure of personal information[213] in connection with commercial activities, and applies to any "organization" involved in commercial activities, regardless of its size. PIPEDA establishes a set of ten principles that companies must follow when processing personal information.[214]

- *Accountability.* A company is responsible for the personal information it collects and controls. The company must designate an individual within the company who will oversee and be responsible for compliance with PIPEDA.
- *Identifying Purposes.* The company must identify the reasons it collects the information, either before, or simultaneous with, the collection of the personal information.
- *Consent.* Where appropriate, the company must seek consent of the individual in processing, storing, and collecting the personal information. Consent must be explicit when the information is of a sensitive nature, but more mundane categories of personal information may only require implied consent. Explicit consent could be acquired orally or through a check-off box, for instance.
- *Limiting Collection.* Only personal information that is necessary for its stated purpose can be collected, and must be collected lawfully.
- *Limiting Use, Disclosure, and Retention.* Personal information cannot be used for a purpose other than the intended purpose of collection, unless the individual has consented to the exception or such alternate use is required by law. Further, personal information must be kept only as long as necessary for the fulfillment of the intended purposes.
- *Accuracy.* Personal information must be accurate, complete, and up to date.
- Safeguards. Personal information must be secured and adequately protected, according to the level of sensitivity of the data. Security safeguards may include

  (1) physical measures (locked filing cabinets, restricting access to offices, alarm systems);

  (2) technological tools (passwords, encryption, firewalls, anonymizing software); and/or

  (3) organizational controls (security clearances, limiting access on a need-to-know basis, staff training, confidentiality agreements).[215]
- *Openness.* A company must make available its privacy policy and reveal how it collects, stores, and processes personal information.
- *Individual Access.* An individual who requests must be given the opportunity to access relevant personal information, and must get the opportunity to correct any inaccurate information.

212. Personal Information Protection and Electronic Documents Act, 2000, c.5 (Can.) (assented to Apr. 13, 2000) (hereinafter PIPEDA).

213. "Personal Information" is broadly defined under PIPEDA as "mean[ing] information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." PIPEDA, Part I(2).

214. The ten privacy principles are located at Schedule 1 (section 5) of PIPEDA.

215. *See* A Guide For Businesses and Organizations: Canada's *Personal Information Protection and Electronic Documents Act*, www.privcom.gc.ca/information/guide_e.asp.

Since January 1, 2004, PIPEDA applies to organizations across the Canadian marketplace, but in some provinces that have enacted a provincial data protection law, an organization will be subject to the provincial law instead of PIPEDA. Such laws include Quebec's personal information protection act, "An act respecting the protection of personal information in the private sector" (popularly known as the "Quebec Act"),[216] as well as the Alberta Personal Information Protection Act[217] and the British Columbia Personal Information Protection Act.[218] However, should any personal information cross a border as part of a commercial transaction, the company will then be subject to PIPEDA. When in doubt and confronted with conflicting federal or provincial regulations, a company should adhere to the higher standard.

Since January 1, 2004, PIPEDA has regulated the processing of personal information through international or interprovincial borders. The European Union has anointed PIPEDA as providing an adequate level of data protection. Therefore, personal data may be freely transferred between a European Union member state and Canada.

§ 24:5.5 China

Communist China's data privacy laws are, at best, sparse. The Chinese constitution refers indirectly to privacy, seeming to guarantee privacy rights in the home and for correspondence.[219] But China does not have sufficient legal infrastructure comprehensively to protect individual privacy. It has passed a few sector-specific privacy laws:

- The Criminal Law Code imposes up to a year in prison on those who violate citizens' "rights of communication freedom"[220] and up to three years on those who illegally search a residence.[221]
- The General Principles of Civil Law[222] prohibits insults, libel, and damage to reputations.
- The Law on the Protection of Minors[223] prohibits collecting "personal secrets" of minors.

China currently offers no Internet-related data protection law, and in fact China is recognized as the world leader in governmental monitoring and censoring of citizens' Internet use.[224] However, in 2003, China participated in the Electronic Commerce Steering Group's APEC Data Privacy Subgroup,[225] a partnership among Asian countries that may have alerted the Communist Party to international privacy concerns.

§ 24:5.6 Colombia

Colombia is yet another South American country that spells out broad personal privacy rights in its constitution. Article 15 grants Colombians a right to

- personal and familial privacy;
- a protected reputation;
- protection of personal correspondence and other personal communications; and
- access to documents in public and private databases—and aright to correct them.[226]

216. Act Respecting the Protection of Personal Information in the Private Sector (Québec Act), R.S.Q., ch. P-39.1 (Can.).
217. Personal Information Protection Act, S.B.C. 2003, ch. P-6.5 (Can.).
218. *Id.* ch. 63.
219. Constitution of the People's Republic of China, XIAN FA arts. 37, 38, 39, 40 (1982) (P.R.C.), *available at* http://english.people.com.cn/constitution/constitution.html.
220. Criminal Law of the People's Republic of China, art. 252, *available at* www.colaw.cn/findlaw/crime/criminallaw1.html
221. *Id.* art. 245.
222. General Principles of Civil Law art. 10 (P.R.C.); *see* Liu Junhai, *Chinese Business and the Internet: The Infrastructure for Trust*, www.civillaw.com.cn/en/article.asp?id=360.
223. Law on the Protection of Minors, 1991 (P.R.C.), *available at* www.unescap.org/esid/psis/population/database/poplaws/law_china/ch_record009.htm.
224. *See, e.g.*, Joseph Kahn, *China Says Web Control Follows the West's Lead*, N.Y. TIMES, Feb. 15, 2006, at A6 col. 5.
225. *See* Asia Pacific Economic Cooperation's website, www.apec.org.
226. Constitución Política de la República de Colombia de 1991 [Constitution], tit. II, *available at* http://pdba.georgetown.edu/Constitutions/Colombia/col91.html.

Colombian Constitutional Court decisions since 1992 hold South American's "habeas data" right implicit in the constitution.[227] Otherwise, no Colombian statute lays out comprehensive constitutional privacy rights, and only a few laws offer specific privacy protections:

- 1990 Decree 1900[228] and 2002 Resolution 575 make telecommunications secret.
- 1999 Law No. 527[229] regulates some forms of electronic commerce. Nevertheless, Colombia is not seen as pervasively enforcing privacy rights; violations of even these few privacy laws are considered widespread, and no data privacy bureaucracy exists to enforce privacy rights.[230]

§ 24:5.7 Costa Rica

Costa Rica has no data privacy statutes, but its constitution protects the right to "intimacy." And the constitution's article 24 was recently amended to refer to personal data[231]—but rather than offer a self-executing right, that amendment obliquely refers to a yet-to-be-enacted law that will spell out what infringements are invasions of privacy.

Accordingly, several privacy bills are crawling through Costa Rica's Assembly. Most propose amendments to Costa Rica's Law of Constitutional Jurisdiction[232] to incorporate a Brazilian-style "habeas data" principle. Another is even broader: A bill introduced in 2005 would create a data privacy bureaucracy.[233]

§ 24:5.8 Hong Kong

Communist China committed to regulating Hong Kong until 2047 under laws completely separate from the mainland's. Hong Kong's "Basic Laws" protect privacy in homes (article 29) and privacy of communications (article 30).[234] More comprehensively, in 1997 Hong Kong passed a Personal Data Ordinance reaching public and private data processors and electronic and nonelectronic records, and launching Hong Kong's own data bureaucracy, the Office of the Privacy Commissioner.[235] That law lays out six "Data Protection Principles":

- collecting personal data
- data accuracy
- retaining data
- using data
- data security
- making data available to individual data subjects[236]

227. *See* Habeas Data, www.ramajudicial.gov.co/csj_portal/assets/HABEAS%20DATA.doc.
228. Decreto No. 1900 de 19 de Agosto 1990, Por el Cual Se Reforman las Normas y Estatutos Que Regulan las Actividades y Servicios de Telecomunicaciones y Afines [Telecommunications Reform Law], Diario Oficial Año CXXVII N.39507 (Colom.), *available at* www.sic.gov.co/Normatividad/Decretos/Decreto%201900-90.php; Resolución No. 575 de 2002 (Colom.), *available at* www.crt.gov.co/Documentos/Normatividad/ResolucionesCRT/00000575.pdf.
229. Ley No. 527, Aug. 21, 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [Electronic Commerce Data Regulation Law], Diario Oficial No. 43.673 (Colom.), *available at* www.secretariasenado.gov.co/leyes/L0527_99.HTM.
230. *See* Privacy International, *Columbia* (Nov. 16, 2004), www.privacyinternational.org/article.shtml?cmd[347]=x-347-83506.
231. Constitución Política República de Costa Rica [Constitution], *available at* www.asamblea.go.cr/proyecto/constitu/const2.htm.
232. Law No. 7128, Aug. 18, 1989, Law of Constitutional Jurisdiction (Costa Rica); *see* Privacy International, *Costa Rica*, at fn.4, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83508.
233. Data Protection Bill 15.178, Protección de la Persona frente al Trata-miento de sus Datos Personales (Costa Rica); *see* Esteban Arrieta Arias, *Crearán Agencia para la Protección de Datos Personales*, LA PRENSA LIBRE, Feb. 8, 2005, *available at* www.prensalibre.co.cr/2005/febrero/08/nacionales03.php.
234. The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China, (1990), arts. 29, 30 (H.K.), *available at* www.info.gov.hk/basic_law/fulltext/index.htm.
235. Personal Data (Privacy) Ordinance, (1996) Cap. 486 (H.K.), *available at* www.pco.org.hk/english/ordinance/ordfull.html.
236. Office of the Privacy Commissioner for Personal Data, The Ordinance at a Glance, www.pco.org.hk/english/ordinance/ordglance1.html#dataprotect.

The Hong Kong law goes on to specify other aspects of data protection, define actionable invasions of privacy, and impose penalties.[237] It then prohibits transmitting personal data offshore to countries like the United States without similar data protections, unless (1) the data subject consents in writing to a transfer[238] or (2) the transfer falls under a contract tracking the Privacy Commissioner's model.[239] In addition, Hong Kong passed other statutes implicating data privacy, primarily the 2001 Code of Practice on Human Resource Management[240] and the 2003 Code of Practice on Consumer Credit Data.[241]

§ 24:5.9 India

In 1964, India's supreme court recognized a right to privacy as part of the larger Indian right to "personal liberty" (from the constitution's article 21). But in 1996, the court retrenched, holding (consistent with US jurisprudence) that the constitutional privacy right exists only as against the *public sector*.[242] Beyond the constitution, a number of Indian statutes also affect privacy:

- Telegraph Act of 1885, amended in 2004, regulates certain public telecommunications.[243]
- Information Technology Act[244] regulates electronic commerce, imposing penalties for introducing computer viruses.
- Prevention of Terrorism Act of 2002[245] limits terrorists' privacy rights.

The pending Right of Information Bill of 2004, a proposal that is the closest India would come to a comprehensive privacy law, is broad but would reach only public institutions.[246]

§ 24:5.10 Israel

Israel has a number of laws regulating privacy:

- The Protection of Privacy Law lays out eleven categories of breaches of privacy and regulates processing of personal data in stored databases.[247]
- The Basic Law on Human Dignity and Freedom establishes a broad right to privacy of "the self," the home, personal belongings, and personal written records.[248]
- The Computer Law of 1995 regulates interceptions of computerized data.[249]
- The Freedom of Information Law of 1998 allows individuals to see to data on file about them in public databases.[250]

237. *Id.*
238. Personal Data (Privacy) Ordinance, (1996) Cap. 486, pt. VI, Matching Procedures and Transfers of Personal Data (H.K.).
239. Office of the Privacy Commissioner for Personal Data, Fact Sheet No. 1, April 1997, Transfer of Personal Data Outside Hong Kong: Some Common Questions, www.pco.org.hk/english/publications/fact1_model.html.
240. *See* Office of the Privacy Commissioner for Personal Data, Code of Practice on Human Resource Management: Compliance Guide for Employers and HRM Practitioners, www.pco.org.hk/english/ordinance/code_hrm.html.
241. Personal Data (Privacy) Ordinance, Code of Practice on Consumer Credit Data, *available at* www.pco.org.hk/english/ordinance/files/CCDCode_eng.pdf.
242. Peoples Union for Civil Liberties (PUCL) v. The Union of India & Another, 18 December 1996, on Writ Petition (C) No. 256 of 1991. India's analysis more or less tracks U.S. Supreme Court jurisprudence on the U.S. Constitution's "penumbral" right of privacy.
243. Indian Telegraph (Amendment) Rules, 2004, Gen. S. R. & O. 220(E), The Gazette of India, Extraordinary, Mar. 26, 2004, Part II, sec. 3, subsec. (i) (India), *available at* www.dot.gov.in/Acts/rules.doc.
244. Information Technology (Use of electronic records and digital signatures) Rules, 2004, Gen. S. R. & O. 582(E), The Gazette of India, Extraordinary, Sept. 6, 2004, Part II, sec. 3, subsec. (i) (India), *available at* www.mit.gov.in/ngnitact.asp.
245. Prevention of Terrorism Act, 2002, Act No. 15 of 2002 (India), *available at* www.satp.org/satporgtp/countries/india/document/actandordinances/POTA.htm.
246. Right to Information Bill, 2004 (India), www.humanrightsinitiative.org/programs/ai/rti/india/national/rti_bill_2004_tabled_version.pdf.
247. Protection of Privacy Law 5741-1981, 1011 LSI 128 (1981), amended by the Protection of Privacy Law (Amendment) 5745-1985 (Isr.); *see* Privacy International, *State of Israel*, www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83794.
248. Basic Law: Human Dignity and Liberty, 1992, 45 LSI 150, sec. 7 (Isr.), *available at* www.knesset.gov.il/laws/special/eng/basic3_eng.htm.
249. *See* Regulation of criminal activities on the Internet in Israel, Report by Keren Alony, 25 November 2002, *available at* www.juridicum.su.se/iri/masterIT/vls/rep/it-crime/israel_internetcrime.html.
250. Freedom of Information Law, 5758-1998 (Isr.), *available at* www.police.gov.il/english/Information_Services/Law/xx_5759_1998.asp.

- The Credit Data Service Law of 2002 lets companies that use individuals' credit histories store personal data in a central database accessible to consumers.[251]

There is an Israeli data bureaucracy, the Registrar of Databases (under the Ministry of Justice).[252] The "Privacy Protection Regulations (Transfer of Information Outside the Country's Borders) 2001" law prohibits sending personal data outside Israel unless:

(1) the data subject consents;

(2) the transfer is to a subsidiary; or

(3) the Registrar of Databases has issued written permission.

The Registrar of Databases accepts US data privacy protections as adequate, so these permissions are not difficult to get.

§ 24:5.11 Japan

Japan's supreme court recognized a right to privacy in 1963, by construing article 13 of the constitution ("right to life, liberty and pursuit of happiness as the supreme consideration in legislation") together with article 35 (protection of privacy within the home).[253] In 1998, Japan launched its own data bureaucracy, the Supervisory Authority for the Protection of Personal Data, to oversee businesses handling personal data under Ministry of International Trade and Industry guidelines.[254] By 2000, Japan's Diet had passed a Communications Interception Law on wiretapping and intercepting e-mail;[255] the next year the Diet passed its Internet Provider Responsibility Law on personal data processing of telecommunications service providers.[256]

But none of these laws is comprehensive. The Diet passed a comprehensive data law only in 2003, effective April 2005—the Personal Data Protection Act (PDPA) of 2003.[257] The PDPA outlines basic data protection policies; directs the bureaucracies that protect privacy; regulates businesses processing personal data;[258] and imposes sanctions of up to six months in prison and 300,000 yen for violations.[259] The PDPA covers all businesses with data about 5,000 or more individuals (apparently worldwide), imposing a "purpose of use" mandate requiring each business to publicize exactly how it uses, stores, and processes personal data. The PDPA also requires businesses to prevent unauthorized disclosure, loss, or destruction of personal data. It limits transfers of data to third parties—whether in Japan or abroad—unless the "principal" (data subject) consents. Businesses need to communicate principals' right to opt out.

§ 24:5.12 Mexico

As with so many Latin American countries, Mexico's constitution guarantees a broad-sounding right to privacy:[260] Each Mexican's personal possessions and home are free from being "molested except by virtue of a written order by a proper authority" and all Mexicans enjoy an explicit constitutional right safeguarding privacy in their private communications, their mail—even their run-ins with the law.[261] However, as of 2006, Mexico had never implemented this right by statute. Mexican lawyers regularly tell anyone who asks that their law imposes no significant limits on businesses processing personal data.

The closest Mexico comes to a comprehensive data law is 2003's Federal Law of Transparency and Access to Government Public Information, which aims to pull together a patchwork of lesser data laws.[262] Critics, however, call this law weak. Most of its provisions

251. *See* Privacy International, *State of Israel*, www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83794.

252. *Id.*

253. *See* Privacy International, *Japan*, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83523.

254. *Id.*

255. *See* Martyn Williams, *Japan's Police Gain Right to Tap Phones and E-mail* (Aug. 16, 2000), www.cnn.com, available at *http://archives.cnn.com/2000/TECH/computing/08/16/japan.police.idg/.*

256. PX Newsflash, Apr. 25, 2002, *available at* www.privacyexchange.org/news/archives/nf/newsflash020425.html.

257. Personal Information Protection Act, Law No. 57 of 2003 (Japan); *see* unofficial translation by Proskauer Rose LLP, *available at* www.proskauer.com/hc_images/JapanPersonalInformationProtectionAct.pdf.

258. *Id.*

259. *Id.*

260. Constitución Política de los Estados Unidos Mexicanos [Const.], *as amended*, art. 16, Diario Oficial de la Federacion [D.O.], 5 de febrero de1917 (Mex.), *available at* http://constitucion.presidencia.gob.mx/index.php?idseccion=71&ruta=1.

261. *Id.*

262. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2003 (Federal Public Government Information Transparency and Access Act), *available at* www.ifai.org.mx/test/new_portal/lftaipg.htm.

address government, not the private sector. The law grants few enforceable rights.[263]

§ 24:5.13 Russia

Russia's constitution, like many others, guarantees a broad right to privacy.[264] Russia's version of this right guarantees privacy in personal or family matters and protects reputations, correspondence, and other communications. The constitution promises Russians access to documents directly affecting their rights, and broadly prohibits collecting, storing, using, or disseminating any personal information without consent.[265]

In 1995 Russia passed a law to implement this right, the Federal Law on Information, Informatization, and the Protection of Information.[266] This comprehensive law lays out government's role in protecting data, prohibits processing private information without consent (except under judicial warrant), and grants data subjects access to government documents about them. Supplementing this law are the following:

- Communications Law, on privacy of communications and wiretapping;[267]
- Law of Operational Investigation Activity, on methods of surveillance and protection of privacy;[268] and
- Federal Law of Commercial Secrets, on protection and dissemination of confidential business information.[269]

Although there are over forty Russian laws that in some way address personal or sensitive data, Russia has neither bureaucracies nor tailored judicial procedures to enforce its web of privacy rules. Violations, and privately held databases of private information, are said to be common.

§ 24:5.14 Singapore

Proposed data privacy legislation has languished in the Singapore legislature for many years. As to privacy, Singapore's constitution is silent, and privacy goes largely unregulated in the law—except for quixotic efforts of an obscure privacy bureaucracy tucked within Singapore's Ministry of Finance.[270] Indeed, Singapore's only privacy laws are fleeting mentions in statutes addressing other topics:

- Computer Misuse Act prevents unauthorized interceptions of computer communications.[271]
- Electronic Transactions Act criminalizes certain confidentiality breaches.[272]
- National Computer Board Act establishes a bureaucracy overseeing computer operations.[273]

Singapore's most robust privacy rules are voluntary business efforts, not laws. In 2000, Singapore's Information Communications Board adopted an "E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce" establishing an industry-based National Internet Advisory Board.[274] Late in 2001, Commerce Trust Ltd. launched a

263. Privacy International, *United Mexican States (Mexico)*, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83805.

264. Konstitutsiia Rossiskoi Federastii [Konst. RF] [Constitution], arts. 23, 25; English translation *available at* www.constitution.ru/en/10003000-01.htm.

265. *Id.*

266. Federal Law on Information, Informatization, and the Protection of Information, No. 24-FZ (Feb. 20, 1995) (Russ.), *available at* www.fas.org/irp/world/russia/docs/law_info.htm.

267. Federal Law on Communication, No. 15-FZ (law passed 1995, updated 2004) (Russ.); *see* Privacy International, *The Russian Federation* (Nov. 16, 2004), www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83789.

268. Federal Law on Operational-Search Activities, No. 144-FZ of August 12, 1995 (passed 1998, updated 2001) (Russ.), *available at* www.legislation-line.org/legislation.php?less=false&lid=6005&tid=155; *see also* Privacy International, *The Russian Federation* (Nov. 16, 2004), *supra* note 267, at n.12.

269. Federal Law on Commercial Secrecy, No. 98-FZ (July 29, 2004) (Russ.),English translation *available at* http://moscow.usembassy.gov/bilateral/bilateral.php?record_id=ipr_lawcs. *See also* www.russianlaws.com/newsdetail.aspx?news=1352.

270. Privacy Knowledge Base Singapore Report, *available at* www.privacyknowledgebase.com/document.jsp?docid=REFDPASP#Republic%20of%20Singapore.

271. Computer Misuse Act, cap. 50A (Sing.), *available at* http://agcvldb4.agc.gov.sg/.

272. Electronic Transactions Act, cap. 88 (Sing.), *available at* http://agcvldb4.agc.gov.sg/.

273. National Computer Board Act, cap. 195 (Sing.), *available at* http://statutes.agc.gov.sg/subindex/C.htm (follow hyperlink at "computers").

274. *See* Privacy International, *The Republic of Singapore*, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83777.

Privacy Trust Global Reliability Program,[275] Singapore's personal-data-protection "trustmark" (seal of approval for businesses voluntarily complying with the privacy trust[276]—this program is said to be loosely modeled on the EU Directive and EU/US safe harbor).[277] In 2002, Singapore's National Internet Advisory board proposed a private sector Data Protection Code.

§ 24:5.15 South Korea

Korea's constitution protects Koreans' privacy at home and privacy of correspondence.[278] Laws implementing this right are chiefly the following:

- Protection of Personal Information Maintained by Public Agencies (1994, amended 2002) regulates public sector privacy issues.[279]
- Electronic Transaction Basic Act (1999) regulates e-commerce.[280]
- Act on the Promotion of Information and Communications Network Utilization and Data Protection (2000) regulates private-sector communications industries.[281]
- Framework Act on Electronic Commerce and the Electronic Signatures Act regulates notifying data subjects of data being processed and their rights of access, and regulates identity theft.[282]

Korea's Personal Information Dispute Mediation Committee (under the Ministry of Information and Communications), a step below the civil trial court, offers streamlined resolution of privacy-related disputes.[283]

§ 24:5.16 Taiwan

Taiwan's protection of privacy is chiefly its constitutional freedom of privacy of correspondence[284] plus its 1995 Computer-Processed Personal Data Protection Law (CPPDPL).[285] The CPPDPL plays out two sets of rules, for public and private sectors, inspired by the EU data protection directive and the Organisation for Economic Cooperation and Development (OECD) guidelines on data collection.[286]

The CPPDPL regulates offshore data transmissions, such as to the United States, but allows foreign transmissions by government bodies "in accordance with relevant laws and ordinances."[287] The CPPDPL, though, lets government restrict a business's offshore data transmissions where the data "involve great interest [to] this country," or where the receiving country lacks laws that "adequately" protect personal data.[288] The CPPDPL neglects to define "adequate." Whether the United States offers "adequate protections" by Singapore standards may be unclear.

275. CommerceTrust Ltd. News Release, CommerceTrust launches first Personal Data Privacy Protection Trustmark in Singapore (July 26, 2001), *available at* www.commercetrust.com.sg/010726.html.

276. Commerce Trust Ltd. News Release, The National Trust Council (NTC) Appoints CommerceNet Singapore (CNSG) as the Authorised Code Owner (ACO) for Business-to-Business eBusiness(s) (Mar. 10, 2004), *available at* www.commercetrust.com.sg/040310.html.

277. *See supra* section 24:3.2.

278. CONST. OF REPUBLIC OF KOREA arts. 16–18 (July 17, 1948), *as amended*; English translation *available at* www.oefre.unibe.ch/law/icl/ks00000_.html.

279. Act on the Protection of Personal Information Maintained by Public Agencies, 1994 (S. Korea). The text of the act can be found in SECRETARIAT OF PERSONAL INFORMATION DISPUTE MEDIATION COMMITTEE, KOREA INFORMATION SECURITY AGENCY, PERSONAL INFORMATION PROTECTION IN KOREA, Annex 2 (Nov. 2002), *available at* www.bakercyberlawcentre.org/2003/Privacy_Conf/papers/Day2/Chung.doc.

280. *See* E-Com Legal Guide, *Republic of Korea*, www.bakerinfo.com/apec/koreaapec_main.htm.

281. Act on the Promotion of Information and Communications Network Utilization and Data Protection, 1999 (S. Korea), as amended; unofficial translation Privacy Knowledge Base Republic of Korea, *available at* www.privacyknowledgebase.com/document.jsp?docid=REFDPASP#Republic%20of%20Korea.

282. Framework Act on Electronic Commerce, 1999, Act No. 5834 (S. Korea); *see* Republic of Korea E-Commerce, *Policy: Regulatory Framework for Promoting E-Commerce*, www.ecommerce.or.kr /about/ec_policy1.asp.

283. Republic of Korea E-Commerce, *Policy: Regulatory Framework for Promoting E-Commerce*, www.ecommerce.or.kr /about/ec_policy1.asp.

284. MINGUO XIANFA art. 21 (1947) (Constitution of the Republic of China), *available at* www.oefre.unibe.ch/law/icl/tw00000_.html.

285. Computer Processed Personal Data Protection Law, 1995 (Taiwan) (hereinafter CPPDPL), *see* www.privacyexchange.org/legal/nat/omni/taiwan.html.

286. *See supra* sections 24:1–24:2.

287. CPPDPL, *supra* note 285, at art. 9.

288. *Id.* art. 24.

Violations of the CPPDPL can mean two years in prison or a fine up to NT $40,000.[289] While no Taiwanese data privacy bureaucracy enforces the CPPDPL, other agencies enforce it within their sectors, and the Ministry of Justice oversees government agency compliance.[290]

§ 24:5.17 Thailand

Thailand's privacy statutes are surprisingly sparse for a kingdom with a constitution that talks so tough on the topic: The kingdom's constitution guarantees each Thai's right to personal and family privacy; protects Thais' reputations and rights to communicate among themselves via "lawful" means;[291] and lets Thais get public documents about themselves (as long as their access preserves kingdom security).[292]

The kingdom's Official Information Act is a public-sector "sunshine law" that lets Thais see public data and regulates how kingdom agencies process personal information.[293] Beyond that, it does little to grant privacy rights—although it does empower a bureaucracy, the Official Information Commission, to oversee things. A bill in the legislature, the would-be Privacy Data Protection Law (PDPL), has so far gone nowhere. If passed, the PDPL would cover collection, use, and storage of personal information, and would establish yet another data bureaucracy.

§ 24:5.18 Uruguay

Unlike its South American neighbors, Uruguay enacted a constitution silent on privacy rights (except for a quick mention of privacy in correspondence).[294] Nor has Uruguay enacted any comprehensive data privacy statute. Yet some local laws do offer certain rights:

- Decree Law no. 14.306[295] regulates privacy in tax matters.
- Decree Law no. 15.322[296] regulates privacy in banking (Uruguay used to be called the "Switzerland of South America," and it still attracts deposits from Argentina, Brazil, and elsewhere).
- Decree No. 396/003 regulates personal data protection in the health care system.[297]
- Law No. 17.838 protects personal information for commercial purposes.
- The Habeas Data Law of late 2004[298] rolls out the Latin American "habeas data" concept.
- Articles 296, 297, and 298 of the Uruguayan Penal Code impose penalties for invasions of privacy in communication (interceptions of correspondence and telephone conversations).[299]

289. Id., *available at* www.privacyexchange.org/legal/nat/omni/taiwan.html.
290. Privacy International, *Republic of China (Taiwan)*, (Nov. 16, 2004), www.privacyinternational.org/article.shtml?cmd[347]=x-347-83551.
291. CONST. OF THE KINGDOM OF THAILAND (1997), arts. 34 and 37, *available at* www.parliament.go.th/files/library/b05-b.htm.
292. *Id.* art. 58.
293. Official Information Act, 1997, B.E. 2540 (Thail.), *available at* www.asianlii.org/th/legis/consol_act/oia1997197.pdf.
294. URUG. CONST., *as amended*, art. 28, *available at* www.parlamento.gub.uy/palacio3/index1024.htm (follow "Constitución de la República" hyper-link).
295. Ley No. 14.306, D.O. 6 dic/974 (Uru.), *available at* www.parlamento.gub.uy/leyes/ley14306.htm.296.Ley No. 15.322, D.O. 23 set/982 (Uru.), *available at* www.parlamento.gub.uy/leyes/ley15322.htm.
296. Ley No. 15.322, D.O. 23 set/982 (Uru.), *available at* www.parlamento.gub.uy/leyes/ley15322.htm.
297. Decreto No. 396/003, Historia clínica electrónica única de cada persona(Uru.) *available at* www.elderechodigital.com.uy/smu/legisla/D0300396.html.
298. *See* Se Dictan Normas para la Protección de Datos Personales a Ser Utilizados en Informes Comerciales, e se Regula aa Acción de "HabeasData," Ley No. 17.838, www.presidencia.gub.uy/ley/2004092801.htm.
299. Código Penal, Ley No. 9.155, 4 de diciembre de 1933, tit. XI, cap. III, arts.296–98 (Uru.), *available at* www.unifr.ch/derechopenal/legislacion/uy/cp_uruguay5.pdf.

International Data Protection and Privacy Law

Donald C. Dowling, Jr., the Firm's International Employment Counsel, concentrates his practice on cross-border human resources law issues for multinational employers.

Don is one of two lawyers in the US ranked in the top tier ("Leading") in the only competitive ranking of international labor/employment lawyers, London-based PLC Which Lawyer?, and he is ranked by Chambers as one of the top 34 Labor & Employment lawyers in New York.

Co-Author, Jeremy Mittman, is a practicing lawyer.

The information in this article is for educational purposes only; it should not be construed as legal advice.