Tel Aviv University Law School
Tel Aviv University Law Faculty Papers

Year 2008 *Paper* 95

The EU Data Protection Directive: An Engine of a Global Regime

Michael D. Birnhack*

*Tel Aviv University, birnhack@post.tau.ac.il

The EU Data Protection Directive: An Engine of a Global Regime

Michael D. Birnhack

Abstract

The article explores a unique form of legal globalization, in which one jurisdiction induces other countries to adopt similar legal mechanisms, without coercion, taking advantage of ignorance or abusing political power. The 1995 EU Directive on data protection regulates the collection, processing and transfer of personal data within the EU, with the dual goal of enabling the free flow of data while maintaining a high level of protection. It includes a mechanism which addresses the export of such data. Article 25 stipulates that member states should allow transfer of data to a third country only if the third country ensures an adequate level of data protection. Thus, countries that wish to engage in data transactions with EU member states are indirectly required to provide an adequate level of protection. The article shows that the Directive has had a far greater global impact than thus far acknowledged and that it is currently the main engine of an emerging global data protection regime. Studying the Directive and its actual impact and comparing it to other mechanisms of legal globalization, I conclude that unlike some American scholars who described the Directive as "aggressive", it is better understood as a non-coercive mechanism of soft legal globalization.

THE EU DATA PROTECTION DIRECTIVE: AN ENGINE OF A GLOBAL REGIME

Michael D. Birnhack*

Forthcoming: 24(6) Computer Law & Security Report (2008)

ABSTRACT

The article explores a unique form of legal globalization, in which one jurisdiction induces other countries to adopt similar legal mechanisms, without coercion, taking advantage of ignorance or abusing political power. The 1995 EU Directive on data protection regulates the collection, processing and transfer of personal data within the EU, with the dual goal of enabling the free flow of data while maintaining a high level of protection. It includes a mechanism which addresses the export of such data. Article 25 stipulates that member states should allow transfer of data to a third country only if the third country ensures an adequate level of data protection. Thus, countries that wish to engage in data transactions with EU member states are indirectly required to provide an adequate level of protection. The article shows that the Directive has had a far greater global impact than thus far acknowledged and that it is currently the main engine of an emerging global data protection regime. Studying the Directive and its actual impact and comparing it to other mechanisms of legal globalization, I conclude that unlike some American scholars who described the Directive as "aggressive", it is better understood as a non-coercive mechanism of soft legal globalization.

1. INTRODUCTION

Privacy is a contested legal concept, with several understandings and more misunderstandings, covering distant areas of human activities. Privacy is under constant attacks from many different angles. Despite the criticism, its inherent vagueness, and instability, privacy is a fundamental human right and a hallmark of democracy. This article focuses on the category of informational privacy and examines the emerging global legal regime that attempts to regulate various aspects of personal data. I examine the role of the EU Data Protection Directive of 1995 and show that it has had a far greater global impact than thus far acknowledged, to the degree that it is currently the main engine of the emerging data protection regime. The Directive is evaluated on the background of American criticism, describing it as aggressive. I conclude that the Directive is better understood as a non-coercive mechanism of *soft legal globalization*.

The discussion begins with three challenges of privacy: a theoretical challenge posed by different understandings of privacy, a technological challenge posed by the digital environment, and a legal challenge. I then turn to describe the emerging global data protection regime beginning with the OECD guidelines of 1980, the Council of Europe's Convention, the UN Guidelines, and current efforts by APEC and a group of data commissioners. We shall then turn to the Directive, study its principles, its mechanism for

* Senior Lecturer (Associate Professor), Faculty of Law, Tel Aviv University. I wish to thank Eyal Benvenisti, Guy Mundlak, participants at the Minerva Conference on the Exercise of Public Authority by International Institutions (Tel Aviv, March 11, 2008), participants at the conference on Convergence and Divergence of Law (Tel Aviv, March 24, 2008), participants at teh third LSPI conference (Prague, Sep. 2008) for helpful comments and Nir Servatka and Adi Teper for research assistance. birnhack@post.tau.ac.il

the regulation of data exports, which are followed by exporting legal norms, and studying its impact. The overall scheme is then evaluated.

2. PRIVACY CHALLENGES

Privacy is a relatively new legal right (Warren & Brandies, 1890). It has complex relationship with social norms; it differs from place to place and has a dynamic relationship with technology. Privacy covers the behavior of people in certain places, like the home, it protects their communications and various aspects of other social interactions. In the United States, privacy covers also some individual decisions, such as a woman's decision to have an abortion. In any case and in all places, privacy is not an absolute right, as it often conflicts with other individual rights or public interests. Thus, privacy has a negative reputation in some circles. Privacy limits the power of the State to enforce the law and fight terror; it sets barriers on the free flow of information in the market and limits the ability of businesses to learn about their customers and personalize their commercial interactions; feminists are concerned that privacy re-establishes the private/public distinction and the press is concerned that it limits its freedom. The discussion is narrowed to address three challenges: theoretical-political, technological-commercial, and ultimately, a legal challenge.

2.1. Theory and Politics

Many people in Western societies have strong intuitions about certain data, which they treat as "theirs," consider it to be personal and private and object when it is collected or used without their consent. The first challenge is to figure out the underlying justifications of protecting privacy. Given that there is no theoretical or political consensus on the matter, we encounter different legal approaches to privacy. The divide between the U.S. and the EU is a stark example.

Phrased in a Kantian spirit, the problem is that someone else decides who we are, ripping us of self control. Thus understood, the control of personal data is a matter of human dignity. A person should be treated as a moral, independent agent, capable of deciding his or her own path in life. The seamless collection of data, its accumulation and subsequent processing slowly transfers our personhood to the control of others, usually corporations. Unlike governments, corporations are unelected, are not subject to constitutional constraints and are not obliged to account for their practices.

Framing the interest in controlling personal data as a matter of human dignity shifts the discussion to the realm of human rights. In some jurisdictions, such as Germany or Israel, human dignity is not only a moral reasoning, but a direct legal source, from which courts can derive rights and duties (Basic Law for the Republic of Germany, article 1(1); Israeli Basic Law: Human Dignity and Liberty, sec. 4). In other jurisdictions, the natural legal category for classifying the protection of the interests mentioned above is the right to privacy. However, privacy turned out to be a less than perfect legal home for addressing such concerns.

In the United States privacy evolved in two realms. One, as a constitutional right protecting citizens against governmental encroachment, understood on the background of liberty (Whitman, 2004). In a second realm, privacy emerged as a common law right classified under tort law, but limited to specific and rather narrow categories. Although privacy is not mentioned in the Constitution, the Supreme Court found that there are "zones of privacy" in the Constitution (Griswold v. Connecticut, 1965). The constitutional right to privacy

extends to people in physical places (Katz v. United States, 1967), to their communications (Electronic Communications Privacy Act, 1986) and to decisional privacy (Griswold, 1967). When Americans talk about privacy as a human right, they mostly refer to the private space that the liberal state should allow the citizen, a space where the person is left alone to do what he or she wishes to do without being listed, without being followed, without any need to explain.

Privacy in the private sphere is narrower and limited to several causes of action recognized by common law (Restatement (Second) on Torts; Prosser, 1960). The category of informational privacy is not included in the traditional classification and remains controversial, despite an academic project urging that such a right is recognized (Richards, 2006). U.S. law opted, instead, for a set of specific regulations in specific sectors. For example, federal law regulates the disclosure of financial data, of health-related data, or of videos rented in video stores. Each of these laws and some others apply a set of rules either regulating the collection of data and its uses, or provides the data subjects with rights to be notified by the data collector, to access the data and to amend it.

There are several possible explanations for the American skepticism towards recognizing a general privacy right in information. A legal-historical explanation would point to the development of two distinct meanings of privacy in the public and private spheres. A political explanation would point to the fundamental mistrust of government, which lies at the heart of the constitutional order and diverts attention from the market (Salbu, 2002). A political-economic explanation is that data is highly valued for its role in the market, both as an important element facilitating the efficiency of the market and as a tradable asset in itself. Regulation of data is thus conceived as an unwarranted intervention in the free market (Posner, 1984). Moreover, not only that citizens (or rather, consumers) do not own the data about themselves (Lessig, 2006:228), those who collect the data are considered to be the owners of that data, perhaps even enjoying some property right therein, or the protection of the First Amendment, as the free speech principle covers commercial speech (Cohen, 2000:1408). In most cases, the free market approach trusts the market to provide solutions for its own failures. Thus, if consumers demand that their data is to be secured in the hands of a trusted controller, the controller is likely to provide reasonable data security measures. Self-regulation better achieves, or so is the belief, the goals of governmental regulation without crude intervention. A related argument is that privacy restricts dissemination of information and thus harms free speech interests (Volokh, 2000; Richards, 2005).

The alternative legal home for the regulation of data is a *sui generis* protection, which is not a sub-category of privacy law, but is a close legal neighbor thereto. This is the avenue chosen in Europe. European law has recognized that data is important *per se*, whether it is the government that wishes to collect and process it or private players in the market. The initial focus is not on the identity of the data controller, but on the interests of the data subject. Personal data (defined as information relating to an identified or identifiable person) is understood in terms of human rights with a proprietary tone. The data subject "owns" the data about himself or herself in the sense that the data cannot be taken without following explicit rules, providing the data subject with some rights to follow the data and empowering the data subject as to subsequent uses. Unlike (real or intellectual) property owners who may transfer their rights to third parties, the data subject maintains his or her rights as to the processing of the data, limiting the data controller also after the transfer of

the data. This body of rules forms a separate legal category of data protection, which is derived from privacy and the idea of human dignity.

Accordingly, the first privacy challenge is choosing the best understanding of privacy and informational privacy.

2.2. Technology and Commerce

The emergence of information technologies posed a new challenge to privacy. Digital technology enables the easy collection of data, its processing, mining, and transferring to third parties. Digital data is easy to collect, it is often a by-product of simple technological processes such as surfing the Internet or of commercial transactions. The cost of collecting the data and its storage are lower than equivalent analogue activities. Digital data is precise, in the sense that it is not prone to mistakes, deterioration of format and the like problems which characterize analogue technologies.

Collecting personal data and processing it is attractive to businesses that wish to improve their services, learn more about their customers and better target them. The data accumulated is a valuable asset. Commercial entities can use such data in the aggregate, to figure out the "market's" demand or behavior, or in its particularized form, to figure out patterns of behavior of a specific consumer and personalize their services. Amazon's recommendations or Google's search results are well known examples. A data collector can offer targeted advertisements, tailor-made services or use the data to deny services, such as loans, insurance or employment. Thus, personal data is an important tool in the hands of businesses vis-à-vis both current and potential customers. Hence, the composition of users' digital dossier (Solove, 2004), is a lucrative business in itself. Once the data is obtained, it is an independent asset that other companies (and governments) (Birnhack & Elkin-Koren, 2003) might be interested in acquiring.

Legal recognition of users' privacy rights seem at first sight to conflict with the commercial needs, as the collection and use of personal data carries with it some risks and dangers. One such risk is that the data will be abused by those who access it, either by authorization or not. Data which was consensually provided for one purpose might be used against us in a different context. For example, genetic data about one's risk of suffering from cancer one day might be the basis for an insurance company to deny its service (cf. Bernstein, 2006; Bregman-Eschet, 2006). Data provided to a school about special needs of a student might be referred to at a later date to deny employment. Furthermore, such data can serve various service providers as a proxy to learn about our personal status, age, health condition, race, ethnicity, religion, sexual preferences and perhaps political views. The data might serve to deny us services or products on basis which otherwise would be considered as illegal discrimination. Once a digital dossier is created, we are classified into a socio-economic category and are treated as if all traits of this category apply to us. Classification limits social mobility. A person categorized early on as a member of a lower socio-economic category might find that many doors are closed.

The argument that privacy conflicts with commerce portrays privacy in a dichotomous manner: either it exits or it does not. This is a misguided claim. Recognizing privacy rights in personal data does not mean that a business cannot collect and process the data, but it does entail some obligations on the data processors and providing data subjects with certain rights. The data protection regime is the framework for these duties and rights.

Furthermore, privacy can foster trade and commerce, as it may enhance the trust of users' in the business with which they are transacting.

Accordingly, the second privacy challenge is to enable businesses to collect the data they need for improving their commercial activities, while providing effective guarantees to data subjects, so that they can maintain control over the use of the data in all phases: collection, use, processing and transferring to third parties. This is a balancing challenge.

2.3. Global Law

The previous two challenges combined, produce the third privacy challenge. Given that privacy is understood differently in the U.S., Europe and elsewhere, and that the legal category of informational privacy (or data protection) is not recognized as such in many countries, and given the technological abilities and commercial interests, what should be the legal regime? The challenge is not only theoretical, as data flows across borders, especially in a global economy and global network. The second challenge, of balancing commercial needs with the privacy rights transcends to the global level. Trans-border data flows facilitate international commerce and the provision of services across borders. Whereas previously, trans-border transactions were mostly B2B (business to business), the new opportunities extend to B2C (business to consumer) transactions, immediately raising privacy concerns.

Local laws fall short of handling the challenges. Information easily crosses physical barriers and national borders. There is no checkpoint or customs agent that can stop the data from flowing from one country to another. A data controller who wishes to avoid a local data protection regime could easily set the database and related operations outside that jurisdiction in a "data haven" (Swire & Litan, 1998:26). Surely, not all companies would relocate just for this reason. Some business models, however, are substantially based on collecting personal data. These collectors are the most dangerous, from a data protection point of view and they have sufficient incentives to avoid burdensome regulations by operating from outside the data protection jurisdiction. Thus, in order to protect local data subjects, some sort of mechanism is required to prevent the circumvention of local data protections.

The two goals of facilitating trans-border data flows and protecting privacy seem to conflict, similar to the second challenge. At first sight, it seems that an either/or approach is sensible and that we ("we" as a global society) should choose which of the conflicting values we prefer. A complete ban on trans-border data flow would best protect privacy. The less information about a data subject is processed, the more privacy protection he or she has. The opposite choice, abolishing data protection, would enable full, uninhibited flow of data across-borders to promote free trade and the creation of a global market. The first option is prohibitively expensive and unenforceable. Data is crucial to facilitate transactions and is a valuable commodity in itself. Under a no-data-flow global regime, a multinational corporation would not be able to operate as one unit or a cluster of divisions; individuals would not be able to travel, engage in cross-border transactions or communications. In fact, any visit to a foreign website would leave a trail of data, which under such a hypothetical regime would not be allowed.

The hypothetical scenario caricatures the interest of data subjects. Whether we understand and classify the interest as a right to informational privacy or a *sui generis* interest of data protection, data subjects do not as a general matter wish to halt the collection and

processing of their data. The data protection (or privacy) regime allows the data subject to decide for herself, if, when and under which conditions is she willing to reveal the data, to whom, and for which purpose. The data protection regime envisions data subjects that provide other parties with their personal data, but empowers them so that they can exercise control over various phases of the data stream. This empowerment is apparent in the data protection principles, discussed shortly. Thus, the third privacy challenge is to construct a viable global legal regime that would provide data subjects with control over their personal data and at the same time, allow trans-border flows.

3. THE EMERGING GLOBAL DATA PROTECTION REGIME

Data protection emerged as a new legal field in the early 1970's, separate from privacy law but yet dependent thereupon. The new field followed the growth of information technologies and globalization processes. We can identify several stages in the evolution of data protection laws, corresponding to the three privacy challenges: firstly, the very emergence of data protection laws and the recognition that personal data requires regulation; secondly, a shift from national laws to international legal regimes, and thirdly, a shift from an emphasis on the collection of data and its initial processing to subsequent uses and transfer to third parties, including trans-border transfers.

The initial political interest in data protection was local, in several states. The appearance of automated data systems brought about a dramatic increase in the quantity of data and the possibilities of processing it. The new setting raised concerns about abuse of the data, driven from a human rights perspective. The first manifestations of data protection law emerged almost simultaneously, first in the form of laws in the Land of Hesse in Germany and Sweden (Ware Report, 1973), and in the form of reports of expert committees in Canada (Department of Communications/Department of Justice, 1972; Bennett, 1990), UK (Younger Committee, 1972) and the United Stated (Secretary's Advisory Committee on Automated Personal Data Systems, 1973).

The growing interest then shifted to the international level. The new possibilities of information technologies were recognized and discussed in multinational forums, where the driving force of protecting human rights was accompanied with new reasons for regulation. In 1980 the Organization for Economic Cooperation and Development (OECD) adopted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, and in 1981 the Council of Europe (CoE) adopted a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

As the title of the OECD Guidelines indicates, the shift from the national to the international level highlighted the need for addressing trans-border data flows. The OECD noted that data contributes "to economic and social development" and recognized that trans-border data flow was a competing value to that of privacy (OECD, 1980). Similarly, the CoE noted that it took "account of the increasing flow across frontiers of personal data undergoing automatic processing" and reaffirmed the Member States' "commitment to freedom of information regardless of frontiers." (CoE, 1981).

Both instruments tried to achieve both goals: protecting the interests of data subjects and enabling trans-border data flows. The various laws and proposals of the 1970s included strikingly similar principles that together formed a set of Fair Information Practices (FIPs), though the details varied. The FIPs defined personal data as information relating to an identified or an identifiable individual and required that data is obtained and processed

fairly and lawfully, a general requirement that is then translated into concrete principles: the data quality principle requires that the personal data collected is relevant to the purpose for which they are used and kept for no longer than is required for that purpose; that the data is accurate and kept updated; the limited use principle requires that the data cannot be used for a purpose other than that for which it was collected; the data controller is subject to a duty to provide data security against unauthorized access; the data subjects should have rights to access the data about them and require that the data is deleted if obtained illegally.

The OECD and the CoE paved the way for other international initiatives. In 1990 the UN published Guidelines Concerning Computerized Data Files, which echo the FIPs of lawfulness and fairness in collecting and processing personal data, accuracy, purpose-specification, access and more (UN Guidelines, 1990). On the matter of trans-border data flows, the UN Guidelines adopt a principle of reciprocity. However, these guidelines lack binding force and the procedures for implementing them are left to the initiative of each State.

The early 1990s were time for the EU to enter this field, resulting in 1995 in the Data Protection Directive. It was based on the OECD Guidelines, CoE Convention and the UN Guidelines, but with some important novelties, which will be discussed in the next section.

Post-Directive developments include two initiatives in the Directive's spirit and one somewhat competing option. The Montreux Declaration of 2005 by a group of Data Protection Commissioners from countries which have data protection laws is in the Directive's spirit. The commissioners, preaching to those already converted, announced their interest in working towards adopting a universal convention on data protection. In the same spirit, the OECD has recently reentered the data protection arena and is engaging in new initiatives. The emphasis of a 2007 Recommendation is on cooperation among members in order to foster cross-border data flow while maintaining privacy (OECD, 2007). The recommendation was to "Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation."

The alternative to the Directive is the regional framework of the Asia-Pacific Economic Cooperation (APEC) which in 2004 initiated a Privacy Framework (APEC, 2004). The 21 member economies adopted nine privacy principles that should be applied: preventing harm, integrity of personal information, notice, security safeguards, collection limitations, access and correction, uses of personal information, accountability, and choice. Like the OECD and CoE, APEC's baseline is the dual goals of protecting privacy and enabling information flows. However, while balancing information privacy and business needs, APEC declares its distinctive approach in that it "accords due recognition to cultural and other diversities that exist within its member economies." Accordingly, it allows flexibility in implementing the principles. The APEC privacy framework lacks regulation of cross-border data flows, other than an indirect accountability duty and a 2007 mild proposal for data transfers within APEC. The then-Australian Federal Privacy Commissioner explained that "accountability should follow the data." (Crompton, 2006). This general principle is then translated into more concrete rules, such as that a data controller should obtain the data subject's consent for transferring the data to a third party. APEC's Framework is weaker than the EU Directive and is less ambitious in scope. Thus, not surprisingly, the APEC Framework is subject to criticism (Greenleaf, 2006; Greenleaf, 2008b).

The common feature of all these initiatives is that they are non-binding international instruments, or in international law parlance, *soft law*. Nevertheless, there is a cumulative effect, in that they promote the dissemination of data protection laws, establish a common set of principles and raise awareness. These initiatives are the foundations of a global data protection regime. The brief outline indicates a slow but nevertheless steady process of globalization of data protection standards, composed of the dissemination of data protection laws and their substantive convergence. The most powerful engine of global data protection laws is the EU Directive, to which we now turn.

4. THE EU DATA PROTECTION DIRECTIVE

The EU Directive on Data Protection (1995), which came into force in 1998, is the most comprehensive and successful international instrument of data protection laws (Swire & Litan, 1998; Bennett & Raab, 2006). It is currently the leading force of globalizing data protection. The Directive now binds the 27 member states of the EU and three members of the European Economic Area (Iceland, Lichtenstein, Norway). It focuses on the internal market, *i.e.*, the European market, with important extra-territorial mechanisms, which are the focus here. The Directive includes various mechanisms that attempt to closely track the flow of data: wherever (European) personal data flows, there should be adequate legal protection of that data. The law follows the data flow. Thus far only a handful of countries were found to ensure an adequate level of protection. However, the Directive's impact should be assessed not only according to the official adequacy findings. Evidence shows that it has a growing impact. Its extra-territorial mechanisms succeed where the other initiatives failed: it is not just a declaration or non-binding guidelines. Neither is the Directive a pure unilateral measure and of course, it is not a binding international treaty. It applies a sophisticated, inducing mechanism to spread its gospel.

4.1. Principles

The Directive aims to serve the conflicting goals of protecting data subjects and facilitating free trade, first and foremost within the EU. The Directive explicitly refers to the right to privacy (recitals 2, 9-11, 68, art. 1(1)), alongside economic and social progress and trade expansion (recitals 2, 56) and the free flow of personal data (art. 1(2)). Instead of presenting privacy and free trade as conflicting, the Directive ties them together: "the establishment and functioning of an internal market in which… the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded" (recital 3). Accordingly, the conclusion is that legal barriers on the free flow of data should be removed. Tying together the two conflicting interests managed to avoid the very real conflict between the two goals. Gutwirth offers sharp criticism: "The European Midas is at work again: everything the Commission touches becomes a market." (Gutwirth, 2002:91). The goal of achieving an internal European market was elevated, he argues, to the same level of fundamental human rights and more so, "The concern about privacy is totally subordinate to the market prerogatives." But, Gutwirth acknowledges that the Directive does rely on privacy and concludes that it is ambivalent and ambiguous (Gutwirth, 2002:92, 94).

The Directive requires member states to enact laws that reflect basic data protection principles, which are based on the CoE Convention (recital 11). The core principles (art. 6), are that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; that the data collected is adequate, relevant and not excessive in relation to the

purposes for which they are collected and/or further processed; that it is accurate and, where necessary, kept up to date; that it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Furthermore (art. 7), personal data may be processed only under certain circumstances: if the data subject has unambiguously consented to the processing; if it is necessary for performing a contract to which the data subject is a party or complying with a legal obligation, protecting vital interests of the data subject, or if the processing is necessary for the public interest or for the controller's legitimate interests. The Directive further prohibits the processing of special categories of data (art. 8), such as racial origins, political beliefs or data relating to health or sexuality. The Directive imposes several obligations on the data controller and accords some rights to the data subject: In order to enable the data subject to perform her rights, the data collector should notify the data subject as to the collection and its use (art. 10); the data subject has a right to access the data (art. 12), to object to certain processing (art. 14), and a right not to be subject to an automated decision (art. 15). The controller is obliged to maintain confidentiality (art. 16), and data security (art. 17), and notify the supervisory authority of certain processing (art. 18). Other principles address situations where the data have not been obtained from the data subject (art. 11). One of the obstacles identified by the Directive is the differences between the legal regimes in the different member states (recitals 7-8). The solution is to enable the free transfer of data, but to assure that data is protected across the EU in a similar, high-level (recital 10).

4.2. Exporting Data

In order to address the challenge of regulating the cross-border data flows so to prevent the circumvention of local data protection laws, the Directive applies a multi-option mechanism (Bennett & Raab, 2006:97-104). The Directive permits extra-territorial processing of data under several routes, structured as a main principle, of addressing a country as a whole (art. 25) and then offering a set of exceptions (derogations)(art. 26).

4.2.1. Country Adequacy

Article 25(1) states that: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

The European Commission's determination that a country ensures an adequate level of data protection is a conclusion of an assessment conducted by the Article 31 Committee. The assessment should be made "in light of all the circumstances surrounding a data transfer operation or set of data transfer operations," (art. 25(2); WP 12, 1998). The Commission guided itself to search for a 'core' of substantive data protection principles and procedural/enforcement requirement that compose a minimum requirement, in order to treat a third country as adequate. The WP instructed that the "minimum list should not be set in stone." (WP 12, 1998). The core principles assessed are similar to those found in the Directive. The Commission seeks these principles in the legal system of the assessed country. The procedural/enforcement requirements are sought in the data protection practice: a good level of compliance, with a high degree of awareness among data controllers of their obligations and among data subjects of their rights, and effective, rapid and not expensive avenues of redress available to the data subjects. The WP emphasizes the importance of institutional mechanisms to serve as an independent investigatory organ.

Importantly, the overall instruction of the Directive as interpreted and applied by the Commission is clear (or, perhaps careful) about the guiding criterion for the assessment: it is the degree of risk that the transfer to the third country poses to the European data subject. The official language of the Directive does not purport to impose itself on other countries in an imperialistic manner. It does not speak of any lofty goals of raising the global level of data protection. The declared goal is framed in a rather modest self-interest spirit: adequacy of third countries is important so to protect the interests of European data subjects. However, more ambitious and less modest aspirations are apparent elsewhere (WP 98, 2004:9).

Unlike the early CoE or the OECD, the Directive was clearly drafted with an eye to the way third countries would respond. Thus, the Directive offers a modest threat. If a third country is found not to ensure an adequate level of data protection, member states "shall take the measures necessary to prevent any transfer of data of the same type to the third country in question." (art. 25(4)). This language leaves some interpretive leeway to the member states: what are the necessary measures to prohibit such transfer of data? It is plausible to argue that the measures should be proportional to the inadequate aspects of the third country. Thus, if a third country does not adequately protect medical data, then the limitation on transfer can be narrowed down to such data. Nevertheless, the Directive realizes that an inadequacy finding might raise difficulties and so it allows negotiations with the third country (art. 25(5)). In practice, over the past decade, the EU has not declared any country to have an inadequate level of data protection. Importantly, data collectors operating in inadequate third country would rely on the other avenues of data export, namely the derogations.

Not surprisingly, countries which have strong commercial ties with the EU (EuroStat) are in the first line to adopt the European view of data protection or examining their data protection regime. The country adequacy avenue has been used thus far only in few cases. Adequacy findings were made regarding Switzerland (1999), Hungary (1999, now a member of the EU), Canada (2002), Argentina (2002), Guernsey (2003), the Isle of Man (2003), and Jersey (2008). The Article 29 WP recommended that Faroe Island (2007) is declared adequate. In addition, specific schemes were found adequate, namely the "safe harbor" agreement in the U.S.

4.2.2. Consent

Article 26(1) lists several options which permit the export of personal data to a third country that does not have adequate protection. These options focus on the individual data subject. The first situation is when the data subject gave unambiguous consent to the transfer. Consent is a crucial element of a data protection regime that is based on the notion of human dignity. Once a person authorizes the collection and processing of her personal data, she exercises her autonomy without external interference. Thus, consent is a key deposited with the sole dominion of the data subject. Only the subject can decide if, when, and to what extent to open his or her virtual private sphere to other entities. Consent is a core principle under the notion of "privacy as control," (Westin, 1967) and an overarching theme which ties together various elements of privacy law. Privacy in one's communications, in one's activities in certain places, in his or her decisions—and in one's data, whether highly personal (such as health-related data or sexuality-related data) or trivial data (consumer habits, internet surfing habits)—all should be governed by the principle of consent.

Consent is a highly volatile concept and subject to manipulation (Froomkin, 2000). What suffices as consent? What happens in the post-consent period? What is the cumulative meaning and effect of consent? If collectors of data can easily gain the data subjects' consent, doesn't this mean it is an empty term? The concern is that consent is a hollow promise of control to the data subject. If the concern materializes, then a consent-based conception of privacy is dangerous: instead of a promise of control, it *de facto* means the opposite, surrender of control. The promise of control turns into an illusion, or worse, deceit. For the above reasons, several privacy scholars abandoned the notion of consent as a central pillar of privacy law in general and data protection in particular (Nissenbaum, 2004).

The Directive attempts to deal with the shortcomings of consent by requiring that processing is allowed subject to the data subject's unambiguous consent (art. 7(a)), by allowing member states to prohibit the processing of special categories of data despite one's consent (art. 8(2)), by requiring prior notification of the data subject (art. 10), and by defining consent (art. 2).

However, these attempts to deal with the limits of consent address the collection and processing of personal data within the EU. The extra-territorial rules enable transfer of data to a third country if there is "unambiguous consent." While this term sets a rather high level of consent, especially when read with the general definition of consent (art. 2(h)), it is ambiguous and leaves a loophole: once the data is transferred, it is almost impossible for the EU data subject to enforce his or her rights, if abridged. Local EU law sets a prerequisite for the export, but does not provide effective enforcement beyond the initial point of consent. This limited power is not unusual and reflects the territorial nature of a country's legal system. The difficulty is the ease in which data crosses borders in digital networks. To be sure, this problem is not only a trans-border problem. Countries face the same difficulty within their borders, but a rich legal toolkit can assist in addressing some of these difficulties, such as state-enforcement by a specialized regulatory authority, general law enforcement agencies, as well as private enforcement, by way of civil suits and class actions. While this toolkit is far from perfect, it does provide a reasonable enforcement mechanism within the EU. However, a citizen of the EU lacks the real power to enforce her rights outside the country, especially when the third country at stake does not have an adequate data protection regime. This major deficiency was not left unobserved by the EU (Commission Staff Working Document, 2006).

The Directive further provides additional avenues for exporting data, when the transfer is necessary for the performance of a contract between the data subject and the controller (art. 26(1)(b)), if the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject (art. 26(1)(c)), or if the transfer is necessary in order to protect the vital interests of the data subject (art. 26(1)(e)). Each of these options makes sense, but the same problem identified with consent applies here too: even if the initial transfer is permitted, it is almost impossible for the European data subject to enforce her rights thereafter.

4.2.3. Standard Contractual Clauses

Whereas consent applies to B2C transactions (Business-to-Consumer), the second derogation addresses B2B (Business-to-Business) data flows. This avenue for the transfer of personal data on EU subjects to third countries focuses on the means by which this is

done: the contract between the European data controller and the foreign data controller (Commission Decision, 2001a, 2004), or between the European data controller and the foreign data processor (Commission Decision, 2001b)). A company may request the approval of the EU data protection authorities. Based on article 26(4) of the Directive, the EU Commission authored model contracts ("standard contractual clauses"), aimed to assure an adequate level of data protection. The model contracts reflect data protection principles and articulate several measures which purport to achieve compliance.

Importantly, under this avenue, enforcement is possible since the data exporter, *i.e.*, the data controller who transfers the data to the other party in the third country, serves as a local, European anchor. Thus, for example, under the model contract, the data exporter warrants that he "has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations" under the contract, and the exporter is the address for data subjects' inquiries. The foreign data importer is obliged to follow an extensive list of commitments. A liability rule supplements these commitments, providing the exporter and importer are liable to each other for breaches of the contract, and more importantly, each party is liable to data subjects for damages it causes by any breach of their rights under the contract. The current model contract, as amended in 2004 does not provide joint and several liability, but it provides the parties with incentives to police each other. The data subject has a valid cause of action against the data exporter for failing to do so.

Thus far, this avenue seems to be under-used (Report of the Commission, 2006), and was applied mostly regarding transfer of data on employees from Europe to the U.S. Furthermore, it is likely that the model contracts serve as a ceiling, rather than a floor (Reidenberg, 2006:1133).

4.2.4. Binding Corporate Rules

Another avenue which the Directive (art. 26(2)) offers for permitted export of personal data is offered to multinational corporations in the form of Binding Corporate Rules (BCR), which require European approval. BCRs are a code of conduct adopted and implemented by a multinational corporation regarding the extra-European processing of data. To be approved, the BCR should comply with the Directive's principles (WP 74, 2003).

Most global firms have European offices and activities as well as commercial activities in third countries and are usually interested in ongoing transfers of data between offices around the world. The data might be about employees, consumers or potential consumers. The individual's consent avenue is available, but means that each transaction and each transfer needs to be evaluated separately to assess its adequacy. The "country adequacy" avenue is irrelevant. Thus, the BCR avenue is easier and cheaper than the alternatives (though it surely does have its costs): instead of a costly process of compliance composed of examining numerous transactions, the corporation can receive the EU's approval for its overall privacy policy.

The benefits of BCR may spillover to individuals. An employee working for a multinational firm operating under a BCR in a third country that lacks any data protection regime, will nevertheless enjoy some protections for her personal data. The spillover may also raise the level of protection accorded by the corporation to non-EU personal data. The EU approval can also reduce the data subject's costs of inquiring the privacy policy of a company.

The BCR avenue suffers from several problems. At present the process of approval is rather long, cumbersome and expensive, though there are intense efforts to streamline the process (WP 108, 2005). Second, BCRs are limited in their scope to particular transfers of data which is in the hands of particular corporations. They do not offer a universal solution to all data protection issues. Third, as Reidenberg argued, the multinational firms are likely to push for a lower level of data protection (Reidenberg, 2006:1134). Fourth, BCRs might conflict with local laws in the many jurisdictions in which the corporation acts. For example, some countries require private firms to transfer certain kinds of data to the government for security reasons (Birnhack & Elkin-Koren, 2003). Fifth, enforceability and compliance are difficult to achieve. The EU attempts to address some of these difficulties by turning to the individual's unambiguous consent (WP 74, 2003). Lastly, implementation within the multinational company is yet another difficulty, especially given the dynamic nature of global business. The contents of the BCR and the EU's approval process attempt to address these issues, though the core difficulties of enforcement, compliance and the approval process are major limitations of this avenue (WP 68, 2003).

4.3. Global Impact

In 1997, Colin Bennett observed that "Nowhere has the Data Protection Directive been the sole reason for another country's passing a data-protection law. On the other hand, it has certainly been one important influence." (Bennett, 1997, 2001:110). A decade after the Directive entered into force, it is time to acknowledge that it has had a wider global impact than thus far acknowledged. We should not examine only the few formal adequacy findings, but search for informal, sometimes subtle, impact. There is sufficient evidence to determine that the Directive has become not only a source of comparative law or a source of inspiration, but an effective mechanism to raise the level of data protection worldwide and that it is doing so better than other mechanisms. What follows is a survey of such evidence.

4.3.1. Australia

In 2006 Australia, a member of both the OECD and APEC launched a thorough study of its data protection regime, undertaken by the Australian Law Reform Commission, which published a 1995 page-long discussion paper in 2007 (ALRC, 2007). The discussion paper includes numerous references to the EU Directive, alongside references to the OECD Guidelines, the CoE Convention and the APEC Framework. These references serve both as a comparative source, *i.e.*, pointing to various policy mechanisms and learning from the European experience, but there are also several direct discussions of the European adequacy requirements. In fact, the ALRC acknowledged that "One of the main drivers behind the *Privacy Amendment (Private Sector) Act 2000* (Cth) was to facilitate trade with European countries by having the *Privacy Act* deemed adequate for the purposes of the EU Directive." (ALRC, 2007:28.131). However, the EU's Article 29 WP reviewed the 2000 legislation and found it could not be deemed adequate. The main points of dispute are that the Australian Act excluded small businesses and employee records, that it did not provide sufficient corrections rights, *i.e.*, the data subject's right to require that the data about her is accurate and the regulation of sensitive data (Waters, 2003). Since then, Australia amended its law, continued its negotiations with the EU and is currently assessed for its adequacy (ALRC, 2007:28.139).

The ALRC report reveals some of the considerations behind the interest in the EU's approval, namely, a European finding that Australia ensures an adequate level of data protection. The first and most influential consideration focuses on the commercial interests

of the Australian market: "In order to ensure that Australian organisations are not disadvantaged in the international market, Australia must be able to meet the international community's expectations of privacy protection." (ALRC, 2007:28.121). The Law Institute of Victoria was more explicit: "If we do not comply with the EU directive, Australian businesses are going to be impacted in terms of the extent to which they can work offshore and deal with other jurisdictions." (ALRC, 2007:28.145). An interesting consideration discussed is symbolic significance. The proponents of Australian adequacy argued that a European finding will provide an important signal about the seriousness it attributes to data protection (ALRC, 2007:28.145). On the other hand, the flexibility of the EU Directive, which offers alternative avenues for exporting personal data from the EU, seems sufficient for some market players and the Australian Office of Privacy Commissioner (ALRC, 2007:28.137). A further consideration against adequacy is that the data protection regime in Europe itself is somewhat inconsistent and that compliance with the Directive (especially registration) is expensive. The ALRC followed the Australian government in working towards adequacy and proposed several amendments to the law, to bring it closer to such a European finding (ALRC, 2007:28.149).

4.3.2. Hong-Kong

Hong Kong, a member of APEC, has been negotiating with the EU its adequacy status (Privacy International, 2006). The motivation for introducing data protection laws was clearly commercial. The former Privacy Commissioner noted that "Hong Kong economy could not afford to be competitively disadvantaged by not having a legal data protection regime that met the requirements of the EU Directive." (Tang, 2003). The economic interest should be read on the background of a global economy and more specifically, the global digital economy. The Commissioner noted that "The perceived value and benefits of electronic commerce has become the driving force behind the quest to seek compatibility." Interestingly, the introduction of data protection law in Hong Kong was an entirely new concept in a region "without a deeply rooted sense of privacy awareness." Thus, the impact of the EU Directive is not only in countries which have had some sort of data protection laws, but to new territories.

4.3.3. Israel

Classified as a developing, high-income country, Israel was invited in May 2007 to open discussions for joining the OECD. Israeli law chose the European understanding of privacy long ago (Birnhack, 2007), as reflected in its Privacy Protection Act enacted as early as 1981, which includes a comprehensive data protection regime. Thus, the law recognizes a general right to privacy, which covers also informational privacy. The law, later accompanied by a constitutional right to privacy (Basic Law, 1992), reflects most of the European data protection principles, including notice, purpose limitation, rights of access and correction accorded to data subjects and duties imposed on data controllers, such as data security, confidentiality and limits on onward transfers.

A recent expert committee recommended a series of amendments (Schofman, 2007). The Committee reaffirmed the Israeli choice of the European understanding of privacy rather than the American view. Other than a comparative source, the motivation was explicitly stated: to avoid limitations on cross-border data flow as a result of different standards of data protection. In its many recommendations, the Committee generally followed the European model and stated the interest in narrowing gaps between Israeli law and EU law. Thus, for example, the Committee recommended that personal data be defined according to the European criterion of identification; that the data protection regime is extended to cover

manual databases, in addition to the already regulated automatic processing systems, reasoning, *inter alia*, the EU Directive. The Directive was referred also in the context of the independent status of the Database Registrar. The Committee advised the Israeli government to initiate an adequacy assessment by the EU, which has followed this advice (Birnhack & Dumortier, 2007).

4.3.4. Japan

Japan, an OECD and APEC member, was early to identify the economic importance of data protection. A 1998 governmental report heavily relied on the then rather new EU Directive as a source of inspiration but also as a policy target – to be recognized as adequate (MITI, 1998). In 2005 Japan enacted a new data protection law, the Personalized Information Protection Law (PIPL), which includes the basic data protection principles, such as notice, consent before disclosing to third parties, purpose limitation, security controls, rights of access and correction and the establishment of a network of data commissioners in each governmental office. This law was deliberately modeled after the EU Directive (Privacy Laws & Business, 2005).

4.3.5. South Africa

Classified by the World Bank as an upper-middle-income economy, South Africa is also examining the introduction of data protection laws. A discussion paper published by the Law Reform Commission in 2005 contains numerous references to the Directive (SALRC, 2005), and set as an explicit objective to ensure that the legislation provides an adequate level of data protection in terms of the Directive. The discussion paper is the basis of a bill, currently being drafted by SALRC.

The motivation in introducing data protection laws that fit the EU standard lies in international trade. SALRC noted that "Privacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends and expectations, information privacy or data legislation will ensure South Africa's future participation in the information market, if it is regarded as providing "adequate" information protection by international standards." (SALRC, 2005:iv). The commercial interest is phrased not only as a carrot, but also as a stick: "Those countries that refuse to adopt adequate data privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data." (SALRC, 2005:4.1.24). In the absence of data protection laws, there are specific examples of South African businesses which conduct business relations with Europeans that were forced to set data processing centers in Europe. Another economic interest is that an adequate data protection regime can attract data processing centers to South Africa.

An interesting consideration discussed by the SALRC is its position vis-à-vis African countries which do not have data protection laws and are unlikely to have such laws in the near future. The concern was that adopting a high-level data protection law, while satisfying the EU, would raise obstacles when trading with African countries. SALRC resolved this by pointing to the other avenues of cross-border data transfers, as provided in the Directive and by noting that "Trade with African countries will be more difficult than with Europe since adequacy will have to be established in each particular transfer. This is, however, the status quo at the moment and this position can not be ascribed to the effects of the information protection legislation." (SALRC, 2005:7.24(2)) The South African choice

is thus to adopt a comprehensive data protection law, structured on the Directive's principles (SALRC, 2005:5.3.3).

4.3.6. Other countries

There are reports of other countries changing their data protection laws with a clear eye to the EU Directive, both as a source of inspiration and with an express interest in an adequacy determination. Several Latin American countries, **Chile, Colombia, Mexico** and **Uruguay** are now seeking an "adequacy declaration" (Privacy Laws & Business, 2008b). **China** has been discussing several proposals, based on an expert committee report. The draft is reported to be influenced by the EU Directive (Greenleaf, 2008a). **Dubai**, the first Arab country to enact a data protection law (2007), closely modeled its law on the EU Directive (Michael, 2007). **India** introduced several rules in its Information Technology Act 2000 and later discussed—and withdrew—a data protection law, based on EU principles (Holder & Grimes, 2007; Privacy Laws & Business, 2003), though a European analysis of India's personal data protection was unfavorable (CRID, 2006). **New Zealand** has a comprehensive data protection law and has been negotiating its adequacy status with the EU (Privacy International, 2007). In the **Philippines**, the Information Technology and E-Commerce Council proposed a data protection law intended to adhere to the EU standards (Holder & Grimes, 2007:704). **Singapore** too is considering a new law (Lehdonvirta, 2004). The **Turkish** parliament is discussing a new data protection bill, which is reported to be part of Turkey's application to join the EU Privacy Laws & Business, 2008a).

4.3.7. Interim Conclusion

The above overview indicates that the EU has managed to raise concrete interest in various countries of various economic statuses to adopt data protection laws (or amend existing laws) so to adhere to the EU's standards. The process is slow and faces local resistance and political attempts to search for less burdensome alternatives. The APEC Framework is an example of such a (regional) attempt, though it is unlikely to prevail (Greenleaf, 2006:17). As the evidence shows, countries seek the EU's stamp of approval for several reasons. The main reason is their own commercial interest, so to enable easier data transfers between their local industries and the EU. A related interest is to facilitate domestic data processing business. A second important interest mentioned is that adhering to the European standard carries symbolic political capital. Developing countries see the European stamp of approval as an invitation to join the club of progressive, modern countries. Interestingly, privacy and data protection are not explicitly mentioned as reasons for adopting the EU standards.

The most important exception to this picture is the United States, Europe's largest trade partner, which does not share the European philosophy of data protection, a gap that is not easy to bridge.

4.3.8. The EU and the US

The data protection divide between the U.S. and the EU was bound to clash. Unlike some of the countries surveyed above, the U.S. does not need the European symbolic approval.

In 2000 after several years of discussions, heated at times, a magical solution was found, at least in theory. The EU Commission and the U.S. Department of Commerce established a safe harbor scheme for American corporations. U.S. firms are invited (but are not obliged) to join the safe harbor. The Safe Harbor is a data protection program, where the firms commit to undertake certain responsibilities regarding personal data. Being voluntary, there

is no state regulation or direct interference in the market and no First Amendment concerns are raised. The contents of the scheme satisfied the EU, which declared it to be "adequate," as if it were a third country (Commission Decision, 2000). From a European point of view, a firm that joins the project can do business with EU data subjects as long as it follows the safe harbor principles.

The principles of the safe harbor are derived from the duty to treat personal data fairly and lawfully and reflect the FIPs which appear in many of the international instruments: these include *notice*, *choice* (data subject would have an opt-out choice regarding the disclosure of their personal data to third parties and an opt-in choice regarding sensitive information); onward transfer; access; security; data integrity; and enforcement.

Enforcement is achieved indirectly. A firm that joins the safe harbor is required to self-certify annually to the Department of Commerce that it adheres to the program and publish a privacy policy statement to that effect. The Federal Trade Commission (FTC) has the power to investigate false presentation. Thus, if an American firm breaches its data protection commitments, it cannot be sued in the U.S. for breach of privacy or data protection rules, as there are no data protection duties inscribed in law, but if the firm joined the safe harbor, the FTC can investigate its public statements and determine whether they were unfair and deceptive.

Thus, the safe harbor creates a multi-layered legal scheme, where self-regulation is indirectly overseen by the state (the FTC's oversight of deceptive presentations), to reach a level which in its substance, satisfies the EU. The framework aims to offer U.S. firms a cheaper way to comply with the EU requirements, *i.e.*, cheaper than obtaining the unambiguous consent of every data subject in every transaction and at the same time, it offers European data subjects the same level of protection that they enjoy at home.

At the time of writing there are 1415 organizations enrolled in the safe harbor. The framework has been examined in a special Implementation Study in 2004 and was criticized on a number of levels (Reidenberg & Bygrave, 2004). First, on the enforcement front, it was pointed that the FTC's power allows an interpretive leeway as to the term "deceptive practices," and applies only to commercial transfers of data. Secondly, other key concepts in the Safe Harbor framework either lack clarity or are not fully commensurate with the Directive's definitions. Third, there are many implementation problems on the substance of the principles and their form.

The safe harbor scheme was intensely challenged in recent years, in two cases: the PNR and SWIFT disputes. In both cases, the background was the events of 9/11 and the dramatic increase in global attention to terrorism. The EU has also responded to the urging need to combat terrorism and its 2002 Directive on Privacy and Electronic Commerce emphasized that it does not address issues of national security (Privacy Directive, 2002). However, despite the shared interest in fighting terror, each continent took a different approach. In the context of personal data, one of the main channels undertaken by the Americans was for the government to utilize data which is held in the private sector. Financial data, data on reading habits, internet browsing and much more are attractive sources for security-based data mining. The PNR and SWIFT are cases of public-private, security oriented "handshake" (Birnhack & Elkin-Koren, 2003).

In the first case, the U.S. amended the Aviation and Transportation Security Act so that airlines flying into the U.S. should enable the U.S. Government (now the Department of Homeland Security - DHS) to have access to the Passenger Name Record (PNR), which includes flight-related data as well as personal data relating to the particular passenger, such as credit card data, special meals (indicating religion or health). Several years of discussions between the U.S. and the EU followed (WP 87, 2004), during which an agreement was reached, according to which the DHS should implement various data protection measures, such as limiting the kinds of data collected, limiting onward data transfers and limiting the use of the data to counter terrorism. A specific adequacy finding followed (Commission Decision, 2004), but in 2006 the European Court of Justice annulled the adequacy finding and required that the agreement with the U.S. is terminated (Court of Justice, 2006). An interim agreement between the U.S. and the EU followed (WP 132, 2007), and then, in 2007, a long-term agreement (WP 138, 2007).

In the second case, the U.S. Department of Treasury (UST) required SWIFT (Society for Worldwide Interbank Financial Telecommunication), a Belgium-based bank transfer organization that handles billions of financial transactions annually, to provide data from its U.S. mirror processing center. The U.S. subpoenas followed the 9/11 events and were complied by SWIFT. Only in 2006 the data transfer was exposed by the media. The Article 29 WP responded swiftly, finding that SWIFT failed to respect the Directive and that the transfer of data to the UST was a serious breach (WP 128, 2006). The WP announced that SWIFT made "hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years without effective legal grounds and without the possibility of independent control by public data protection supervisory authorities constitutes a violation of the fundamental European principles as regards data protection and is not in accordance with Belgian and European law." (Art. 29 Press Release, 2006). The real parties to the dispute were the EU and the U.S. government. Negotiations followed, and in 2007 an agreement was reached, according to which the U.S. government undertook representations, limiting the purposes for which the UST would access data to counter terrorism purposes; and provide other data protection guarantees (German Presidency Press Release, 2007).

The PNR and SWIFT cases illustrate the Atlantic divide regarding data protection. The solutions are a compromise for both sides. From a data protection perspective, the EU managed to insert its principles into the policy calculations and mindset of reluctant counterparts.

5. CONCLUSION

The overall picture of data protection laws and initiatives around the world over the past four decades indicates a slow, but steady expansion. At the time of writing, 77 countries have already enacted data protection laws of some sort, or are part of regional initiatives (CoE, EU, APEC), or have made steps to join them. Additional countries are examining their data protection status (*e.g.*, South Africa). The efforts of the OECD, UN and the Data Commissioners to foster data protection principles are beginning to show fruit. There are more and more dots on the global map of data protection laws, to the extent that a line can be drawn between them. Indeed, the dots are far from being identical: different jurisdictions regulate data protection in different ways, have different preferences as to the mode of regulation, provide different remedies and numerous other variations. But, there is a general framework in place, which is now being pulled (or perhaps pushed) by the EU's engine.

The EU Directive has a central role in adding new dots on the global map and connecting them to a unified picture. The adequacy mechanism spreads the European view more efficiently than the non-binding OECD Guidelines, CoE Convention, or UN Guidelines, and no doubt that it is more effective than the APEC scheme, which currently lacks any serious treatment of data flows outside the APEC economies. This does not mean that the Directive is perfect; it is not. Clarifications are needed, enforcement lacks, and the very concept of data flows, merits re-examination. Describing data as "flowing", as if it were a physical object, does not reflect the global digital environment, in which data *is* everywhere. For the Directive to export its principles more efficiently the adequacy assessment process should be streamlined and perhaps a "model law" would be helpful.

Perhaps not surprisingly, two American scholars, Tim Wu and Steven Salbu, separately characterized the Directive as "aggressive." Wu added that it is "notorious," and compared the adequacy mechanism of the Directive's article 25 to the American unilateral measures in the intellectual property context, namely the "special 301" review. Both "are efforts to set up a closed community for which entry is premised on good behavior. Both are ultimately efforts to make the laws of other countries more like the EU or the United States, respectively." (Wu, 2008). Salbu wrote that the Directive's "data flow provisions are a threat to nations outside the European Union." (Salbu, 2002:689). He emphasized the unilateral aspect of the Directive and complained that the Directive limits global negotiations as the basic requirements applied by the EU to third countries are non-negotiable. Reidenberg was less critical and observed that "in effect, Europe, through the European Directive, has displaced the role that the United States held since the famous Warren and Brandeis article in setting the globally privacy agenda." (Reidenberg, 2001:737). Canadian political scientist, Colin Bennett termed the Directive's effect on third countries as "penetrative," and predicted that it will have a more coercive effect on third countries (Bennett, 2001:111).

It is my opinion that the Directive's mechanism is not aggressive, either in the books or in practice, neither is it similar to the measures undertaken in the intellectual property context. The Directive is not coercive, as no country is forced to change its laws to fit the Directive. No country is obliged to seek the EU's stamp of approval. The Directive offers a "green route" to those countries that are deemed adequate, but does not direct the inadequate countries to any "red route." In fact, most countries have not earned the adequacy status and the EU has not to this day imposed any limitations on the data flows to these countries, instead it started negotiations with these countries. The Directive enables, as discussed earlier, that personal data is exported by obtaining the data subject's consent, or by using contractual clauses, or by the BCR avenue.

The result of the EU's mechanism is that while its initial purpose was to ensure the local, European data protection regime, the extra-territorial mechanisms have, by definition, an externality. Those who prefer to make their local decisions themselves, *i.e.*, exercise sovereignty, in an isolated manner, view it as a negative externality and fight back, whereas data protection and privacy supporters view this as a positive externality.

References

1. APEC Privacy Framework (2005). <http://tinyurl.com/2kvpr2> [last visited 4.6.2008].
2. Article 29 Working Party (2006). Press Release of November 23, 2006. <http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf> [last visited 4.6.2008].

3. Australian Law Reform Commission (ALRC)(2007). Review of Australian Privacy Law, Discussion Paper (2007).<http://www.austlii.edu.au/au/other/alrc/publications/dp/72/DP72.pdf> [last visited 4.6.2008].
4. Basic Law for the Republic of Germany (Germany).
5. Basic Law: Human Dignity and Liberty (Israel).
6. Bennett, C. (1990). The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing, Canadian Public Administration Volume 33, 551.
7. Bennett, C.J. (1997, 2001). Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?. In Agre, P.E., & Rotenberg, M. (Eds.) Technology and Privacy: The New Landscape. Cambridge, MA: MIT Press.
8. Bennett, C.J., & Raab, C.D. (2006). The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge, MA: MIT Press.
9. Bernstein, G. (2006). The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy. Connecticut Law Review Volume 39, 241-295.
10. Birnhack, M., & Elkin-Koren, N. (2003). The Invisible Handshake: The Reemergence of the State in the Digital Environment. Virginia Journal of Law & Technology Volume 8, 6.
11. Birnhack, M.D. (2007). Control and Consent: The Theoretical Basis of The Right to Privacy. Law and Government in Israel Volume 11, 9-73 [Hebrew].
12. Birnhack, M.D., & Dumortier, F. (2007). Israel Asks EU to Assess its DP Law for Adequacy. Privacy Laws & Business Volume 86, 10-11.
13. Bregman-Eschet, Y. (2006). Genetic Databases and Biobanks: Who Controls our Genetic Privacy? Santa Clara Computer & High-Technology Law Journal Volume 23, 1-54.
14. Canada, Department of Communications/Department of Justice (1972). Privacy and Computers.
15. Cohen, J.E. (2000). Examined Lives: Informational Privacy and the Subject as an Object, Stanford Law Review Volume 52, 1373-1438.
16. Commission Decision (2000). Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215 , 0007-0047.
17. Commission Decision, (2001a). Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC.
18. Commission Decision, (2001b). Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC.
19. Commission Decision (2004). Decision 2004/915/EC of 27 December 2004 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.
20. Commission Staff (2006). SEC(2006) 95, Working Document, on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC)(2006). <http://tinyurl.com/3x5bz6> [last visited 4.6.2008].
21. Council of Europe (1981). Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data Council of Europe, European Treaty Series No. 108
22. Court of Justice (2006). Joined cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States.
23. CRID, (2006). First Analysis of the Personal Data protection Law in India, Final Report. <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf> [last visited 4.6.2008]
24. Crompton, M. (2006). APEC Information Privacy Framework (Review, Impact, and Progress), Keynote Speech at APEC Symposium on Information Privacy Protection in E-Government and E-Commerce. In Symposium proceedings. <http://tinyurl.com/36dsur> [last visited 4.6.2008].
25. Electronic Communications Privacy Act (1986). Pub. L. 99-508, 100 Stat. 1848, codified as 18 U.S.C. §2510.
26. European Communities, Commission (1995). Directive 95/46 EC of the European Parliament and of 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. Official Journal of the European Communities 23 November 1995; L281:31.
27. European Communities, Commission (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
28. European Court of Justice, (2006). Joined cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States.
29. Eurostat data. <http://tinyurl.com/356q4v> [last visited 4.6.2008].
30. Froomkin, A.M. (2000). The Death of Privacy. Stanford Law Review, volume 52. 1461-1543.
31. German Presidency Press Release, (2007). <http://www.eu2007.de/en/News/Press_Releases/June/0629BMFswift.html> [last visited 4.6.2008].
32. Greenleaf, G. (2006). Asia-Pacific Developments in Information Privacy Law and its Interpretation, Privacy Issues Forum. Wellington, NZ <http://tinyurl.com/2n9cch> [last visited 4.6.2008].
33. Greenleaf, G. (2008a). China Proposes Personal Information Protection Act. Privacy Laws & Business Volume 91, 1-6.
34. Greenleaf, G. (2008b). APEC's Privacy Pathfinders – A Dead End for Consumers?. Privacy Laws & Business Volume 91, 12-14.
35. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).
36. Gutwirth, S. (2002). Privacy and the Information Age. Raf Casert translator. Oxford, UK: Rowman & Littlefield Publishers.
37. Holder, J.T., & Grimes, D.E. (2007). Government Regulated Data Privacy: The Challenge for Global Outsourcers. Georgetown Journal of International Law Volume 38, 695-711.
38. Israel Ministry of Justice, (2007). Report of the Committee for the Examination of Legislation Relating to Databases (Schofman Report).
39. Katz v. United States, 389 U.S. 347 (1967).
40. Killion, M.U. (2004). China's Foreign Currency Regime: The Kagan Thesis and Legalification of the WTO Agreement. Minnesota Journal of Global Trade Volume 14, 43-89.
41. Lehdonvirta, V. (2004). European Data Protection Directive: Adequacy of Data Protection in Singapore, Singapore Journal of Legal Studies 511.
42. Lessig, L. (2006). Code version 2.0. New York: Basic Books.
43. Michael, J. (2007). Dubai Adopts First DP Law in an Arab Country. Privacy Laws & Business Volume 86, 1-4.
44. Ministry of International Trade and Industry, Japan (MITI)(1998). Japan's Views on the Protection of Personal Data.
45. Montreux Declaration, (2005). The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities (2005). <http://tinyurl.com/2gmfe6> [last visited 4.6.2008]
46. Nissenbaum, H. (2004). Privacy as Contextual Integrity, Washington Law Review Volume 79, 119-157.
47. OECD (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
48. OECD (2007). Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.
49. Posner, R.A. (1984). An Economic Analysis of Privacy. In F.D. Schoeman (Ed.). Philosophical Dimensions of Privacy: An Anthology (pp. 333-345). Cambridge: Cambridge University Press.
50. Privacy International (2007). Report of 2006. <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559512> [last visited 4.6.2008].
51. Privacy Laws & Business (2003). India to Water Down Privacy Plans. Volume 70, 8.
52. Privacy Laws & Business (2005). Ministers Give Guidance on Japan's New DP Law. Volume 77, 6.
53. Privacy Laws & Business (2008a). Turkey Applies to DP Club; DP Part of EU Application. Volume 93, 1.

54. Privacy Laws & Business (2008b). Latin American Calls for International Standards. Volume 94, 8.
55. Prosser, W.L. (1960). Privacy (A Legal Analysis). California Law Review Volume 48, 383.
56. Reidenberg, J.R. (2001). E-Commerce and Trans-Atlantic Privacy, Houston Law Review Volume 38, 717-749.
57. Reidenberg, J.R. (2006). The Simplification of International Data Privacy Rules, Fordham International Law Journal Volume 29, 1128-1138.
58. Reidenberg, J.R., & Bygrave, L.A. et al (2004). Safe Harbour Decision Implementation Study <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf> [last visited 4.6.2008].
59. Restatement (Second) on Torts (U.S.).
60. Richards, N.M. (2005). Reconciling Data Privacy and the First Amendment, UCLA Law Review Volume 52, 1149-1222.
61. Richards, N.M. (2006). The Information Privacy Law Project. Georgetown Law Journal Volume 94, 1087-1140.
62. Salbu, S.R. (2002). The European Union Data Privacy Directive and International Relations, Vanderbilt Journal of Transnational Law Volume 35, 655-695.
63. Schoffman Report (2007). Ministry of Justice, Committee for the Examination of Legislation Relating to Databases.
64. Secretary's Advisory Committee on Automated Personal Data Systems, 1973).
65. Solove, D.J. (2004). The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press.
66. South African Law Reform Commission (SALRC)(2005). Discussion Paper 109, Project 124, Privacy and Data Protection. <http://www.doj.gov.za/salrc/dpapers.htm> [last visited 4.6.2008].
67. Swire, P.P., & Litan, R.E. (1998). None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive. Washington D.C.: Brookings Institution Press.
68. Tang, R. (2003). Implementing Data Privacy Principles: How Are Governments Making it Work in the Real World?. <http://www.pcpd.org.hk/english/infocentre/apec_feb03.html> [last visited 4.6.2008].
69. United Nations, (1990). Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990. <http://www.unhchr.ch/html/menu3/b/71.htm> [Last visited 4.6.2008].
70. United States, Ware Report (1973). Computers and Privacy: The Reaction in Other Countries, <http://aspe.os.dhhs.gov/datacncl/1973privacy/appenb.htm> [last visited 4.6.2008]
71. Volokh, E. (2000). Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, Stanford Law Review Volume 52, 1049-1124.
72. Warren, S., & Brandies, L. (1890). The Right to Privacy, Harvard Law Review Volume 4, 193.
73. Waters, N. (2003). The European Influence on Privacy Law and Practice. Privacy L. & Policy Reporter, 2. <http://www.austlii.edu.au/au/journals/PLPR/2003/2.html#fn12> [last visited 4.6.2008].
74. Westin, A. (1967). Privacy and Freedom. Atheneum.
75. Whitman, J.Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty, Yale Law Journal Volume 113, 1151-1221.
76. Working Party 12 (1998). Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection Directive. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf> [last visited 4.6.2008].
77. Working Party 68 (2003). Working Document on on-line authentication services. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf> [last visited 4.6.2008].
78. Working Party 74 (2003). Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers

<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf> [last visited 4.6.2008].
79. Working Party 87 (2004). Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP). <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf> [last visited 4.6.2008].
80. Working Party 98 (2004), Strategy Document, <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp98_en.pdf> [last visited 4.6.2008]
81. Working Party 108 (2005). Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf> [last visited 4.6.2008].
82. Working Party 128 (2006). Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf> [last visited 4.6.2008].
83. Working Party 132 (2007). Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp132_en.pdf> [last visited 4.6.2008].
84. Working Party 138 (2007). Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_en.pdf> [last visited 4.6.2008].
85. Wu, T. (in press). The International Privacy Regime. In Chander, A., Gelman, L., Radin, M.J. (Eds.), Securing Privacy in the Internet Age. Stanford University Press.
86. Younger, K. (1972). Report of the Committee on Privacy. London, UK.