Journal of Air Law and Commerce

Volume 67 | Issue 1 Article 6

2002

Attacks on America - Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada

Ruwantissa Abeyratne

ATTACKS ON AMERICA—PRIVACY IMPLICATIONS OF HEIGHTENED SECURITY MEASURES IN THE UNITED STATES, EUROPE, AND CANADA

RUWANTISSA ABEYRATNE*

I. INTRODUCTION

AS A CONSEQUENCE of the attacks on the United States, which took place on September 11, 2001, aviation paid the irrecoverable cost of having aircraft used as weapons of mass destruction. An inevitable corollary to these incidents would be heightened security at airports and airline check-in counters. Some of these security measures would undeniably include the use of advance passenger information and biometric identification methods. The latter is part of Simplified Passenger Travel (SPT), which is a process introduced largely to alleviate the usual drawn-out process of passenger clearance at airports that had become characteristic of air travel. The system anchors itself on the use of a smart card holding relevant information of the passenger that can be swiped through a machine, giving instant clearance.[1]

Hand in hand with the use of a smart card is the practice of exchanging Advance Passenger Information (API), whereby a passenger' s information is provided, in advance of his arrival, to the immigration and customs authorities of the destination State, particularly to be used for deciding whether that passenger shall be admitted to the State or not. The customs authorities conceived the idea of an API system. They identified the need to address the increased risk posed by airline passengers in recent years, especially regarding drug trafficking and other threats to national security. In some locations, this need to en-

* The author is a senior official at the International Civil Aviation Organization (ICAO). He has written this article in his personal capacity.

[1] For more information on the use of the smart card, see Ruwantissa I.R. Abeyratne, *The Automated Screening of Passengers and the Smart Card—Emerging Legal Issues,* 23 AIR & SPACE LAW 3, 3–7 (1998).

hance controls, combined with the growth of air passenger traffic, began to place a severe strain on the resources of customs and immigration services, resulting in unacceptable delays in the processing of arriving passengers at airports. As a means of addressing the twin objectives of improved compliance and faster clearance of low-risk passengers, customs and immigration officials envisioned a system in which passengers' identification data could be sent to the authorities and processed against computer databases while the aircraft was in flight.

Article 29 of the Convention on International Civil Aviation (the Chicago Convention) requires every aircraft engaged in international navigation to carry certain documents, including "a list of [passenger] names and places of embarkation and destination."[2] Annex 9 to the Convention, on facilitation of air transport, specifies that *presentation* of the passenger manifest document shall not normally be required, but, if *information* is required, it is to be limited to the data elements included in the prescribed format, *i.e.,* names, places of embarkation and destination, and flight details.[3]

When this standard was adopted, it contemplated the passenger manifest as a paper document, either typed or written, and delivered by hand. The concept of limiting the amount of information to be collected and delivered to that which is essential to meet the basic objectives of safety, efficiency, and regulatory compliance applies equally to modern electronic-data interchange systems, such as API, where additional, but not unlimited, data can be transmitted to the authorities in exchange for a more efficient clearance operation. It is widely recognized that in any system involving the exchange of information, automated or not, it is the collection of data that creates the major expense. Increases in data-collection requirements should result in benefits that exceed the additional costs.

As the airlines and control authorities progress in their refinement of the system and improvement of its performance, passenger clearance times for transoceanic flights (which, prior to use of API, frequently involved delays in excess of two hours) have been reduced to averages well below the recommended goal of forty-five minutes stipulated in Annex 9. In addition to

---

[2] Convention on International Civil Aviation, Dec. 7, 1944, art. 29, 61 Stat. 1180, 15 U.N.T.S. 295 [hereinafter Chicago Convention]. A copy of the Convention may be obtained from the ICAO, Doc. 7300/8 (8th ed. 2000).

[3] Chicago Convention, *supra* note 2, at Annex 9, std. 2.7 (emphasis added).

this improvement in efficiency, the control authorities have realized an enhancement of their enforcement efforts, due to the fact that the receipt of information in advance gives them more time to process passenger information and make better decisions regarding their inspection targets and the appropriate level of control.

The data transmitted by the airlines to immigration and customs authorities of recipient States include details contained in the machine-readable zone of a passport,[4] plus specific data concerning the inbound flight, such as airports of departure/arrival, flight number, and date. An Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) message format is used to transmit the data by EDI. The system works well, but is very demanding in terms of requirements for high levels of thoroughness and accuracy of data provided. Unlike cargo shipments, each of which is processed for clearance on its own track, passengers must pass through immigration and customs as a "flight" and are interdependent with respect to the time it takes to clear them. If data on too many passengers is missing, the whole group is delayed, and so are the flights of passengers arriving after them.

There is an ongoing tug-of-war between the airlines and immigration/customs services over airline-system performance standards versus short clearance times (facilitation benefits) provided by the authorities. But the reality is that the higher the data quality, the faster the clearance can be accomplished. So, the airlines must meet a certain standard of data quality in order to get "blue lane" treatment.

One issue that emerges as important in the API process is that the data required must be collectable by machine or already contained in the airline's system. Manual collection and data entry at the check-in desk for a scheduled flight is time-consuming and prone to errors and, therefore, is not acceptable. Fortunately, most travellers now hold machine-readable passports (MRPs) and, as a result, manual input need only be done on an exception basis. Participation in API must be done in conjunction with a measurable improvement in facilitation. The authorities concerned must also ensure an improvement in security.

---

[4] For details on the machine-readable passport and its development in the ICAO, see Ruwantissa I. R. Abeyratne, *The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject*, 27 ANNALS AIR & SPACE L. 1, 1–31 (1992).

Another important issue that could be raised within the umbrella of API pertains to the privacy of the data subject. This article examines the status of the privacy of individuals in North America and Europe and how it will be impacted by the security measures that may be taken in the field of aviation in the wake of the September 11 attacks on the United States.

The data subject, like any other person, has an inherent right to his privacy. The subject of privacy has been identified as an intriguing and emotional one.[5] The right to privacy is inherent in the concept of liberty, and is the most comprehensive of rights and the right most valued by civilized man.[6] However, this right is susceptible to erosion, as modern technology is capable of easily recording and storing dossiers on every man, woman and child in the world.[7] The data subject's right to privacy is brought into focus by Alan Westin, who defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information is communicated to others."[8] There are four rights of privacy relating to the storage and use of personal data:

1. The right of an individual to determine what personal information to share with others, and to control the disclosure of such data;
2. The right of an individual to know what personal data are disclosed, what data are collected, and where such data are stored;
3. The right to dispute incomplete or inaccurate personal data; and
4. The right of those who have a legitimate right to know personal data in order to maintain the health and safety of society and to monitor and evaluate the activities of government.[9]

---

[5] John B. Young, *A Look at Privacy*, *in* PRIVACY 1 (John B. Young ed., 1978).

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

[7] As far back as 1973 it was claimed that "ten reels each containing 1,500 metres of tape 2.5 [centimetres] wide could store a twenty-page dossier on every man, woman, and child in the world." R.V. Jones, *Some Threats of Technology to Privacy*, *in* PRIVACY & HUMAN RIGHTS 139, 158 (A. H. Robertson ed., 1973) (presented at the Third International Colloquy about the European Convention on Human Rights, Brussels, Sept. 30–Oct. 3, 1970).

[8] ALAN F. WESTIN, PRIVACY AND FREEDOM 7, 124 (1967).

[9] Gordon C. Everest, *Nonuniform Privacy Laws: Implications and Attempts at Uniformity*, *in* COMPUTERS AND PRIVACY IN THE NEXT DECADE 141, 142 (Lance J. Hoffman ed., 1980).

It is incontrovertible therefore that the data subject has a right to decide what information about himself to share with others and more importantly, to know what data are collected about him. This right is balanced against the right of a society to collect data about individuals so that the orderly running of government is ensured.

II. ISSUES OF PRIVACY

The role played by technology in modern-day commercial transactions has affected a large number of activities pertaining to human interaction. The emergence of the information superhighway and the concomitant evolution of automation have inevitably transformed the social and personal lifestyles and value systems of individuals, created unexpected business opportunities, reduced operating costs, accelerated transaction times, facilitated accessibility to communications, shortened distances, and removed bureaucratic formalities.[10] Progress notwithstanding; technology has bestowed on humanity automated mechanisms, devices, features, and procedures that intrude into personal lives of individuals. For instance, when a credit card is used, it is possible to track purchases, discovering numerous aspects about that particular individual, including food preferences, leisure activities, and consumer credit behavior.[11] In a similar vein, computer records of an air carrier's reservation system may give out details of a passenger's travel preferences, *inter alia*, seat selection, destination fondness, ticket-purchasing dossier, lodging keenness, temporary address and telephone contacts, attendance at theatres and sport activities, and whether the passenger travels alone or with someone else.[12] This scheme

---

[10] *See generally* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Clarendon Press 1984) (1949).

[11] For a detailed analysis of the implications of credit cards with respect to the right of privacy, see STEVEN L. NOCK, THE COSTS OF PRIVACY: SURVEILLANCE AND REPUTATION IN AMERICA 43 (1993).

[12] The paramount importance of airline computer reservation system records is reflected in the world-renowned cases of *Libyan Arab Jamahiriya v. United Kingdom* and *Libyan Arab Jamahiriya v. United States* regarding the 1988 PanAm 103 accident at Lockerbie, Scotland, where the International Court of Justice requested air carriers to submit to the Court the defendants' flight information and reservation details. *See* International Court of Justice News Release 99/36, Questions of Interpretation and Application of the 1971 Montreal Convention Arising from the Aerial Incident at Lockerbie (July 1, 1999), *available at* http://www.icj-cij.org/icjwww/ipresscom/ipress1999/ipresscom9936_iluklus_19990701.htm. Similarly, Arthur R. Miller describes the significance of airline computer reservation system records when dealing with federal, state, local, and other types of

of things may well give the outward perception of surveillance attributable to computer devices monitoring individuals' most intimate activities and preferences, leading to the formation of a genuine "traceable society."[13]

The main feature of this complex web of technological activity is that the enormous amount of personal information being handled by such varied players from the public and private sector may bring about concerns of possible "data leaks" in the system, a risk that could have drastic legal consequences affecting an individual's rights to privacy.

At the international level, privacy was first recognized as a fundamental freedom in the Universal Declaration of Human Rights.[14] Thereafter, several other human rights conventions followed the same trend, granting individuals the fundamental right of privacy.[15] The preeminent concern of these international instruments was to establish the necessary legal framework to protect the individual and his inherent right to the enjoyment of a private life.

---

investigations where these dossiers could provide valuable information. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 42 (1971).

[13] *See* GINI GRAHAM SCOTT, MIND YOUR OWN BUSINESS: THE BATTLE FOR PERSONAL PRIVACY 307 (1995); DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 20 (1983). *A contrario* to the argument supported in this thesis (that the advancement of technology directly affects the intimacy of individuals), United States Circuit Judge Richard Posner favors the idea that other factors, such as urbanization, income, and mobility development have particularly weakened the information control that the government has over individuals: this denotes that individuals' privacy has increased. *See* Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 409 (1978).

[14] The text reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." *See Universal Declaration of Human Rights*, G.A. Res. 217A (III), U.N. GAOR, 3d Sess., at art. 12, U.N. Doc. A/810 (1948).

[15] *See International Covenant on Civil and Political Rights*, G.A. Res. 2200A (XXI), art. 17, U.N. GAOR, 21st Sess., Supp. No. 16, at 52, U.N. Doc. A/6316 (1966); *American Declaration on the Rights and Duties of Man*, O.A.S. Res. XXX, art. 5, *International Conference of American States*, 9th Conf., OAS Doc. OEA/Ser.L/V/I. 4 Rev. XX (1948); American Convention on Human Rights, Nov. 22, 1969, art. 11, 1144 U.N.T.S. 123; *International Convention on the Protection of the Rights of Migrant Workers and Members of Their Families*, G.A. Res. 158, U.N. GAOR, 45th Sess., Agenda Item 12, art. 14, U.N. Doc. A/RES/45/158 (1991), *reprinted in* 30 INT'L LEGAL MATERIALS 1519 (1991); *Convention on the Rights of the Child*, G.A. Res. 25, U.N. GAOR, 44th Sess., Agenda Item 108, art. 16, U.N. Doc. A/RES/44/25 (1989), *reprinted in* 28 INT'L LEGAL MATERIALS 1456.

Privacy represents different things for different people.[16] The concept *per se* has evolved throughout the history of mankind: first, as the original anti-intrusion approach, which defended an individual's property and physical body against unwanted invasions and intrusions; then manifesting in whom to associate with; later enlarging its scope to include privacy as the individual's decision-making right;[17] and culminating in the control over one's personal information.[18] The conceptual evolution of privacy is directly related to the technological advancement of each particular period in history.

The right of privacy, as enunciated by United States Judge Thomas M. Cooley, was the right "to be let alone" and was a part of a more general right to one's personality.[19] This idea was given further impetus by two prominent young lawyers, Samuel D. Warren and Louis D. Brandeis, in 1890.[20] Before this idea was introduced, privacy reflected primarily a somewhat limited, "physical" property or concept. By contrast, "information privacy," where individuals determine when, how, and to what extent information about themselves shall be communicated to others, in other words, the right to control information about

---

[16] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 33 (1995); Paul A. Freund, *Privacy: One Concept or Many, in* PRIVACY 182 (J. Roland Pennock & John W. Chapman eds., 1971).

[17] In this case, the U.S. Supreme Court acknowledged the right of women to have abortions based on the grounds that the federal government could not interfere within her *decisional privacy* sphere. *See* Roe v. Wade, 410 U.S. 113, 153 (1973). *See also* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 49 (1997). *See also* WILLIAM ZELERMYER, INVASION OF PRIVACY 16 (1959).

[18] In a remarkable case concerning the legality of a national census scheduled by the authorities, the German Constitutional court connected the individuals' liberty and the personal data processing of the intended census, to rule that if the individuals do not know for what purposes and who is collecting the data, that situation will eventually create an abdication of the individual's rights to the processor's command, *which cannot be tolerated in a democratic society. See* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data,* 80 IOWA L. REV. 445, 447–48 (1995); *see also* STEVEN HOFFER, WORLD CYBERSPACE LAW 8-2 (2000); Ruth Gavison, *Privacy and the Limits of the Law,* 89 YALE L.J. 421, 423 (1980).

[19] *See* Warren & Brandeis, *supra* note 6, at 195 (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888)).

[20] The definition of privacy as the "right to be let alone" is often erroneously attributed to Warren and Brandeis. *See* Warren & Brandeis, *supra* note 6, at 195. Additionally, the concept of privacy as "the right to be let alone," as well as "the right most valued by civilized man," was embraced by U.S. courts in the landmark dissenting opinion of Justice Louis D. Brandeis in *Olmsted v. United States,* 277 U.S. 438, 478 (1928).

oneself,[21] is a cornerstone of modern ideas of privacy. With the development of computer capabilities to handle large amounts of data, privacy has been enlarged to include the collection, storage, use, and disclosure of personal information.[22] The notion of informational privacy protection, a typically American usage, has been particularly popular both in the United States and Europe, where the term "data protection" is used.[23]

The German Bundesverfassungsgericht judicially embraced self-determination in the right to protect one's privacy in 1983.[24] The Supreme Court of the United States followed this trend by adopting the principle of privacy self-determination in *Department of Justice v. Reporters Committee for Freedom of the Press.*[25]

It must be borne in mind that privacy is not an absolute, unlimited right that operates in isolation.[26] It is not an absolute right applied unreservedly to the exclusion of other rights. Hence, there is frequently the necessity to balance privacy rights against other conflicting rights, such as the freedom of speech and the right to access information, when examining individuals' rights *vis-à-vis* the interests of society.[27] This multiplicity of interests will prompt courts to adopt a balanced approach when

---

[21] *See* WESTIN, *supra* note 8, at 368. For a similar conceptualization of privacy, see Charles Fried, *Privacy: Economics and Ethics, A Comment on Posner* 12 GA. L. REV. 423, 425 (1978).

[22] *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995).

[23] The term "data protection" has been translated from the German word *datenschutz*, referring to a set of policies seeking to regulate the collection, storage, use, and transfer of personal information. *See* COLIN J. BENNET, REGULATING PRIVACY 13 (1992).

[24] In a remarkable case concerning the legality of a national census scheduled by the authorities, the German constitutional court connected the individual's liberty and the personal data processing of the intended census, to rule that if the individuals do not know for what purposes and who is collecting the data, that situation will eventually create an abdication of the individual's rights to the processor's command, which cannot be tolerated in a democratic society. *See* Simitis, *supra* note 18, at 447–48.

[25] 489 U.S. 749, 763 (1989).

[26] *See* Arnold Simmel, *Privacy Is Not an Isolated Freedom, in* PRIVACY 71 (J. Roland Pennnock & John W. Chapman eds., 1971).

[27] *See* ANDREW HALPIN, RIGHTS & LAW: ANALYSIS & THEORY 111 (1997); *see also* Leslie G. Foschio, *Motor Vehicle Records: Balancing Individual Privacy and the Public's Legitimate Need to Know, in* PRIVACY AND PUBLICITY 35 (Theodore R. Kupferman ed., 1990). For a comprehensive study on the conflictive interest between privacy and the mass media and the Freedom of Speech, see DON R. PEMBER, PRIVACY AND THE PRESS 227–249 (1972); Judith B. Prowda, *A Lawyer's Ramble Down the Information Superhighway: Privacy and Security of Data*, 64 FORDHAM L. REV. 738, 769 (1995). *See also* AMERICAN PRESS INSTITUTE J. MONTGOMERY CURTIS MEMORIAL

adjudicating a person's rights, particularly where the interests of a State are involved.

A. Privacy Issues in the United States

It would not be incorrect to recognize the fact that the right of privacy originally evolved in the United States following the appearance of an influential article written by Warren and Brandeis.[28] This article was prompted by the increasing intrusion of the newspaper media, particularly the yellow press, which publicly scrutinized personal issues of Bostonian society in the late 1800s.[29] Although Warren and Brandeis stress the importance of protecting the individual right of privacy against mass-media invasion by suggesting that an independent cause of action under tort law is necessary, the issue remains primarily applicable to private individuals.[30]

The right of privacy brings to bear the need to identify possible scenarios when addressing issues of privacy rights. The United States has a two-pronged approach to the right of privacy:

1) Privacy rights between the individual and the State; and
2) Privacy rights between different individuals.

The former consideration involves both U.S. constitutional law, since indirect references to privacy are found in the Bill of Rights, and federal legislation, including some specific legislation Congress has enacted.[31] The latter is addressed through the law of torts, and is, hence, a governmental matter involving specific legislation regulating certain industries.[32] It should be noted that the United States has adopted the approach of sectoral regulation in terms of privacy, as opposed to the enact-

---

SEMINAR, THE PUBLIC, PRIVACY AND THE PRESS: HAVE THE MEDIA GONE TOO FAR?, 2 (1992).

[28] *See* Warren & Brandeis, *supra* note 6, at 195.

[29] Apparently the concern of Samuel Warren for privacy was born when the emerging Bostonian yellow press scandalized his wife's entertainment activities. *See* MILLER, *supra* note 12, at 170. For a good study on colonial privacy in New England, see DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 164 (1972).

[30] The former Privacy Commissioner of British Columbia, Canada asserted that privacy was originally a *nonlegal concept*. *See* David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. 831, 832 (1991).

[31] The Supreme Court of the United States has strongly affirmed that the U.S. Constitution does not grant privacy rights to private individuals among themselves, thus leading to its resolution to the law of torts. *See* Prudential Ins. Co. v. Cheek, 259 U.S. 530, 543 (1922).

[32] *See* CATE, *supra* note 17; *see also* ZELERMYER, *supra* note 17.

ment of the "omnibus data protection statues" undertaken in Europe.[33] This makes U.S. conceptualization of the right of the privacy admit as little government interference as possible. Three factual bases encompass the rationale for the approach in the United States. First, a large number of Americans believe that their rights can be adequately protected through the implementation of industry codes, norms and business practices, company policies, proper technical network structure, good corporate citizenship through the implementation of guidelines,[34] and perhaps even through contractual arrangements, particularly on the basis that the market has matured sufficiently enough to be self-regulated.[35] This attitude reflects the trust of the American people in the private sector. *A contrario,* numerous commentators and prominent civil liberties groups have expressed profound concerns about whether further government intervention has become necessary.[36] Second, the tremendous power of influential industry lobbying groups strongly opposes any further government intervention with business. United States lobbying groups have direct access to the White House, and thus represent considerably more bargaining power than the individual data subject.[37] Third, the United States favors the free flow of information according to the principles embraced by the First Amendment,[38] based on the premise that the availability of information will be regulated by the marketplace of

---

[33] *See* IAN J. LLOYD, INFORMATION TECHNOLOGY LAW 38 (2d ed. 1997).

[34] For an interesting business guidelines compromise with respect to the privacy of customers, see Direct Marketing Association, *Privacy Promise Member Compliance Guide: Keeping Our Privacy Promise to Consumers, at* http://www.the-dma.org/library/privacy/privacypromise.shtml (last visited July 13, 2000).

[35] *See* Reidenberg, *supra* note 22, at 515.

[36] *See* Joel. R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce,* 14 BERKELEY TECH. L.J. 771, 792 (1999); Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions,* 6 SOFTWARE L.J. 199 (1993); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate,* 49 S.C. L. REV. 847, 860 (1998) (indicating that the U.S. Government, while acknowledging the serious threats to the privacy of consumers, has decided to adopt an industry self regulation approach which conflicts with the EC Directive); Patricia Mell, *A Hitchhiker's Guide to Trans-Border Data Exchanges Between EU Member States and the United States Under the European Union Directive on the Protection of Personal Information,* 9 PACE INT'L L. REV. 147, 182 (1991); Jennifer M. Myers, *Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain, and the United States,* 29 CASE W. RES. J. INT'L L. 109, 146 (1997).

[37] *See generally* JAMES RULE ET AL., THE POLITICS OF PRIVACY (1980).

[38] U.S. CONST. amend. I.

ideas, hence reflecting an enormous trust thereto.[39] In addition, some commentators suggest that excessive protection of personal information would inevitably distort efficient market functions.[40] Therefore, it is unlikely that the U.S. Congress will enact a general, comprehensive set of rules addressing privacy, as prevails in Europe.[41]

Commentators in the United States have identified five dimensions, or categories, of privacy: 1) "Physical Privacy," addressed through issues related to the physical integrity of the individual, originally protected through the tort of trespass to the person;[42] 2) "Decisional Privacy," embraced in the landmark case *Roe v. Wade*,[43] where the U.S. Supreme Court acknowledged the right of privacy to include the right to make one's own decisions about activities related to marriage, procreation, contraception, abortion, family relationships, and education; 3) "Communications Privacy," related to the First Amendment's Freedom of Speech and Association, where an individual is granted the right freely to communicate among peers; 4) "Ter-

---

[39] In this respect, Fred H. Cate has written:

> The U.S. approach to information privacy inevitably results in some harm to individual's privacy, reputations, and sensibilities. But it reflects a constitutional calculation that such harm is less threatening to the body politic than the harm associated with centralized privacy protection, government interference with the information flows necessary to sustain democracies and markets, and the growing ineffectiveness of omnibus legal controls in the face of the widespread proliferation of powerful information technologies.

Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 174, 231 (1999).

[40] *See* Posner, *supra* note 13, at 400; *see also* GRAHAM SCOTT, *supra* note 13, at 307; BURNHAM, *supra* note 13, at 20. *A contrario* to the argument supported in this thesis that the advancement of technology directly affects the intimacy of individuals, U.S. Circuit Judge Richard Posner favors the idea that other factors, such as urbanization, income, and mobility development have particularly weakened the information control that, for instance, the government has over individuals; this denotes that individuals' privacy has increased. *See* Posner, *supra* note 13, at 409.

[41] *See* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 763 (1999) (reviewing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996)).

[42] Originally the law provided a remedy solely for physical interference with the life and property of the individual. *See* MORRIS L. ERNST & ALAN U. SCHWARTZ, PRIVACY: THE RIGHT TO BE LET ALONE 47 (1962).

[43] The Supreme Court of the United States acknowledged the right of women to have abortions based on the grounds that the federal government could not interfere within their *decisional privacy* sphere. *See* Roe v. Wade, 410 U.S. 113 (1973).

ritorial Privacy," setting limits or boundaries on intrusion into a specific space or area of one's property; and 5) "Information Privacy," addressing "control of handling of personal data."[44]

The U.S. Constitution does not include any direct reference to privacy within its text. However, the Bill of Rights addresses the issue indirectly through the First Amendment rights to Freedom of Speech, Press and Association;[45] the Third Amendment relating to the quartering of soldiers;[46] the Fourth Amendment right to be free from unreasonable searches;[47] and the Due Process Clause of the Fourteenth Amendment.[48] Most constitutional issues related to privacy have been dealt with through the Fourth Amendment. Notwithstanding all of this, the recognition of privacy rights within U.S. constitutional law came somewhat late, which is surprising for a nation so involved in recognizing the protection of civil liberties. Individual privacy rights were first recognized under the U.S. Constitution[49] in Justice Louis Brandeis' dissenting opinion in *Olmstead v. United States.*[50] Justice Brandeis energetically pursued the legal ground for protection of the right to privacy against the intrusion of the State into one's personal affairs. However, in *Olmstead,* the U.S. Supreme Court upheld the ruling of the Circuit Court of Appeals for the Ninth Circuit, which had held that obtaining evidence without physically invading constitutionally protected areas (for instance, through wiretapping) did not violate the Fourth Amendment and, therefore, did not constitute an illegal

---

[44] *See* Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union,* 21 LOY. L.A. INT'L & COMP. L.J. 661, 664 (1999).

[45] *See* U.S. CONST. amend. I.

[46] *See* U.S. CONST. amend. III.

[47] The full text of the amendment reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. At the outset, the Fourth Amendment was envisaged as a safeguard to protect private property interests against the abuse of the federal government, a situation that was frequent during colonial times. The concept was later extended to include privacy. *See* DONALD E. LIVELY, LANDMARK SUPREME COURT CASES 127 (1999).

[48] *See* U.S. CONST. amend. XIV.

[49] *See* BERNARD SCHWARTZ, 1 A COMMENTARY ON THE CONSTITUTION OF THE UNITED STATES § 395 (1968).

[50] 277 U.S. 438, 478 (1928).

search.[51] The Court's decision created a requirement of physical invasion, adopting the so-called trespass theory of searches and seizures of tangible property, thereby enlarging the scope of government intrusion in the individual's private life.[52]

The first case where a Constitutional right of privacy was officially recognized by a majority of the U.S. Supreme Court was *Griswold v. Connecticut*,[53] where Justice Douglas, writing for the Court, observed that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . . . Various guarantees create zones of privacy."[54] Justice Douglas' opinion acknowledged the protection of privacy contained in the Bill of Rights, inferring that protection from the applicability of the First, Third, Fourth, Fifth, and Ninth Amendments. The fundamental value of this case lies in the Court's recognition that several parts of the Bill of Rights indirectly refer to and thus protect the right of privacy. Subsequently, the U.S. Supreme Court adopted a broader interpretation of the protection of privacy rights in the landmark case *Katz v. United States*,[55] stating that the Fourth Amendment protects people rather than zones or areas of privacy, leaving behind the trespass tangible requirement previously adopted in *Olmstead*.[56]

---

[51] *Id.* at 478. The same rationale was later adopted in *Goldman v. United States*, 316 U.S. 129 (1942).

[52] *Olmstead* involved the secret activities of alcohol smugglers who were intercepted by the police. The ruling of the Court came when the prohibition of alcohol was at its peak. The Court was likely influenced by the fact that the smuggling of alcohol became a major concern for the U.S. authorities and the media itself. *Olmstead*, 277 U.S. at 455.

[53] *See* Griswold v. Connecticut., 381 U.S. 479 (1965). The case involved the claim of a couple against a Connecticut statute prohibiting the distribution of contraceptive information. The court ruled in favour of the couple, granting the *marital right of privacy*. However, the court failed to define such a right. *See* PROSSER & KEETON ON TORTS 867 (W. Page Keeton et al eds., 5th ed. 1984).

[54] *Griswold*, 381 U.S. at 484. The principle of constitutionally protected areas of privacy was adopted, *inter alia*, in *Silverman v. United States*, 365 U.S. 505 (1961); *Lopez v. United States*, 373 U.S. 427 (1963); and *Berger v. New York*, 388 U.S. 41 (1967).

[55] 389 U.S. 347 (1967). The Supreme Court adopted the same rationale in *Terry v. Ohio*, 392 U.S. 1, 9 (1968).

[56] *Katz*, 389 U.S. at 351, 353. The case involved the wiretapping of a telephone conversation that an individual conducted from a public telephone booth, where a recording device was attached. *See also* CHESTER J. ANTIEAU, 1 MODERN CONSTITUTIONAL LAW 160 (1969).

In the 1979 case of *Smith v. Maryland*[57] the Supreme Court had to address the issue as to whether the installation, at the request of the police, of a pen-register tape[58] at a telephone company for the purpose of listening to a phone conversation of a presumed robber, constituted a search requiring a warrant under the Fourth Amendment. The Court held that when the data subject does not have a "legitimate expectation of privacy," the installation of a pen-register tape for the purpose of monitoring calls does not constitute a search. The Court established the "legitimate expectation of privacy" test as comprising of a two-fold requirement. First, the Court analyzed whether the individual had a legitimate expectation of privacy. If that were the case, the Court then proceeded to examine whether society is prepared to recognize that expectation as reasonable, and whether the individual is entitled to be free from unreasonable governmental intrusion.[59] In a similar approach, Justice Breyer, dissenting in *Bond v. United States*[60] expressed his deep concern about the fact that the "actual expectation of privacy" is a subjective matter, but its determination must be "objectively" reasonable.[61] It is indeed interesting that the "legitimate expectation of privacy test" established in *Smith v. Maryland* places an onerous burden on the individual, who must prove not only infringement of a right, but also the reasonableness of his "legitimate expectation." Additionally, the second component of the aforesaid test confers a significant discretionary spectrum to courts on a case-by-case basis. Under the circumstances, it would be legitimate to consider the level of privacy protection given to the data subject by this precedent, particularly in view of various lower courts' decisions in the United States.[62]

---

[57] 442 U.S. 735 (1979). The same reasoning was applied in *Bond v. United States*, 529 U.S. 334 (2000) and *California v. Ciraolo*, 476 U.S. 207 (1986).

[58] A pen-register tape was later defined as "a device which records or decodes electronic or other impulses which identify the numbers dialled or otherwise transmitted on the telephone line to which such device is attached." *See* 18 U.S.C. § 3127(3) (1994).

[59] *Smith*, 442 U.S. at 740.

[60] 529 U.S. 334, 340 (2000).

[61] *See* JOHN H. F. SHATTUCK, RIGHTS OF PRIVACY 19 (1977).

[62] *See Smith*, 442 U.S. at 735; *Bond*, 529 U.S. at 334; and *Ciraolo*, 476 U.S. at 207. Furthermore, in *United States v. Smith*, 978 F.2d 171 (5th Cir. 1992), involving the interception of cordless phone conversations, the claim was denied on the basis that the plaintiff failed to introduce evidence that his subjective expectation of privacy was reasonable.

Hitherto, all the cases examined herein dealt with general issues of privacy protection in U.S. courts, but contained no direct reference to the implementation of automation devices to collect personal data, as this study pursues. In *Whalen v. Roe*[63] the Supreme Court addressed the issue of whether the State of New York could record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and unlawful market. The Court held in favor of the State and pronounced that there was no invasion of privacy, concluding that the State does have the right to collect such data for public purposes. This case is compelling with respect to issues pertaining to the use of personal data by the State or any government agency.[64]

In *Iacobucci v. City of Newport*[65] the Court of Appeals for the Sixth Circuit upheld the right of the city to request compliance with a fingerprinting ordinance for all bar employees. Accordingly, in *Perkey v. Department of Motor Vehicles*[66] the California Supreme Court was in favor of asserting the right of the State to require individual citizens to provide fingerprints prior to obtaining a license. In *Skinner v. Railway Labour Executives Association*,[67] the U.S. Supreme Court acknowledged that a state regulation compelling the collection and testing of railway employees' urine constituted a "search subject to the demands of the Fourth Amendment." However, in applying the public-interest test to the case in question, the Court considered that the regulation sought to achieve public safety for the benefit of society, an interest that outweighed the individual's expectation of privacy. Then, in *Vernonia School District v. Acton*,[68] the Supreme Court held that a school district's policy authorizing the drug testing of students participating in the district's athletics pro-

---

[63] 429 U.S. 589 (1977).

[64] *See generally*, Amy M. Jurevic, *When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail*, 66 U.M.K.C. L. REV. 809 (1988).

[65] 785 F. 2d. 1354 (6th Cir. 1986). Similar decisions were previously given in *Thom v. N.Y. Stock Exch.*, 306 F. Supp. 1002 (S.D.N.Y. 1969), and *Miller v. N.Y. Stock Exch.*, 425 F. 2d. 1074 (2d. Cir. 1970).

[66] 721 P.2d 50 (Cal. 1986).

[67] 489 U.S. 602 (1989).

[68] 515 U.S. 646 (1995).

grams did not violate the Fourth Amendment because the public interest was best served thereby.[69]

The foregoing cases clearly support the argument that U.S. courts, within the public sphere of the constitutional right of privacy, show a tendency to establish the two-fold test conceived in *Smith v. Maryland*, whereby the individual's expectation of privacy is balanced against the public interest of society. Therefore, it becomes clear that when a federal agency seeks to implement automated devices, such as biometric measurement embedded in a smart card, for the purpose of accelerating the passenger traffic flows, U.S. courts will rarely find a situation where a privacy right under the protection of the Fourth Amendment has been violated, because the public interest is being served.

B. PRIVACY ISSUES IN EUROPE

The conceptual realm of privacy rights in Europe is diametrically opposed to that of the United States. Europe has placed more emphasis on legislative edict in accordance with its long-standing civil-law background, and followed an approach based on predicting the probable consequences of the emergence of particular phenomena, as has been reflected in the enactment of omnibus regulation, rather than letting law evolve as a consequence of judicial experiences.

The European approach to privacy protection is deeply rooted in the reference made to the right of privacy in the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (the European Convention),[70] Article 8 of which establishes privacy as a fundamental human right.[71] Hence, Europe tends to approach privacy as a preeminent concern of humanity where the law should provide as much foreseeable protection as

---

[69] For a comprehensive examination of the conflictive interest between privacy and public safety in drug testing cases, see JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY 125 (1997).

[70] *See* European Convention for the Protection of Human Rights and Fundamental Freedoms (E.T.S. No. 5), Nov. 4, 1950, art. 8, 213 U.N.T.S. 221, 223, *as amended through* Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms (E.T.S. No. 155), entered into force Nov. 1, 1998 [hereinafter Convention of Human Rights and Fundamental Freedoms], *available at* http://www.echr.coe.int/Convention/webConvenENG.pdf.

[71] *See also* David Feldman, *Privacy-related Rights and their Social Value, in* PRIVACY AND LOYALTY 29 (Peter Birks ed., 1997).

possible.[72] With the introduction of the European Convention, numerous European countries began enacting regulation-addressing privacy.[73]

Later, the Council of Europe, pursuant to Resolution 73/22, adopted the *Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data* on January 28, 1981,[74] based on OECD model recommendation guidelines.[75] Although the Convention included only the automated processing of data, leaving manual processing beyond its scope, it set forth

---

[72] The European authorities have long expressed concern about the possible implications to individuals' privacy caused by the advancement of technology. Hence, the Committee of Experts on Human Rights reported in 1970 that the existing legal framework was inadequate to protect privacy rights. *See* LLOYD; *supra* note 33, at 45.

[73] The German State of Hese passed the first legislation in Europe addressing privacy data protection in 1970. Later, Sweden passed the Svenska Datalag (Swedish Data Act) of 1973; Germany enacted the Deutsche Bundesdatenschutzgsetz (Federal Data Protection Act) in 1977; France passed the Loi relative a l'informatique, aux fichiers et aux libertes (Data Protection Act) in 1978; Austria endorsed the Datenschutzgesetz (Data Protection Act), also in 1978; finally Great Britain established the Data Protection Act of 1984. *See* Viktor Mayer-Schönberger, *Trans-Atlantic Information Privacy Legislation and Rational Choice Theory*, 67 GEO. WASH. L. REV. 1309, 1316 & nn.37–41 (1999); *see generally* J.A.L. STERLING, THE DATA PROTECTION ACT OF 1984 (2d ed. 1985); Joan Johnson-Freese, *Seven Years of Swedish Data Legislation—Analysis of Impact and Trend for the Future, in* INFORMATIQUE ET PROTECTION DE LA PERSONNALITÉ 69 (1981); J. VELU, LE DROIT AU RESPECT DE LA VIE PRIVÉE 19 (1974); RAYMOND WACKS, PERSONAL INFORMATION 39 (1989); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989); FRANCOIS RIGAUX ET AL., LA VIE PRIVÉE, UNE LIBERTÉ PARMI LES AUTRES? (1992); FROM DATA PROTECTION TO KNOWLEDGE MACHINES (Peter Seipel ed., 1990); Yves Poullet, *Data Protection between Property and Liberties, in* AMONGST FRIENDS IN COMPUTERS AND LAW 161 (H.W.K. Kaspersen & Anja Oskamp eds., 1990).

[74] *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (E.T.S. No. 108), Jan. 28, 1981, *reprinted in* 20 INT'L LEGAL MATERIAL 377 (1981) [hereinafter *European Convention*]. The EC Commission later recommended that states adopt the aforesaid Convention, understanding that the establishment of a common market calls for an extensive standardization of data processing at the European level. The *rationale* of the European efforts lies in the fact that data protection is desirable because it allows for the free movement of data and information across frontiers and prevents unequal conditions of competition and the subsequent distortion of the common market. *See* Commission Recommendation 81/679/EEC of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981 O.J. (L 246) 31.

[75] *See* COUNCIL OF EUROPE, EXPLANATORY REPORT ON THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (No. 108) (1981); COUNCIL OF EUROPE, NEW TECHNOLOGIES: A CHALLENGE TO PRIVACY PROTECTION? (1989). *See generally* PROTECTION OF PERSONAL DATA USED FOR SOCIAL SECURITY PURPOSES (1986).

the early goals pursued by European authorities, and identified many of the issues that remain relevant in modern legislation. However, the instrument's main flaw lies in the fact that it was ratified by only a small number of countries, and hence failed to achieve a uniform standard degree of privacy protection within Europe.[76] Therefore, the European Commission acknowledged the necessity of taking further actions to achieve such goals by requiring states to harmonize privacy data legislation. Thus, the path was set for the advent of the European Privacy Data Directive.[77]

On October 24, 1995, the European Parliament and the European Council passed Directive 95/46 (EC Directive) relating to the protection of the processing and movement of personal data.[78] The intention of the EC Directive's framers was to equalize the disparity of levels of data protection within Europe, whereby countries such as France and Germany had very comprehensive legislation, while others like Italy and Greece had none. The EC Directive, which came into force in 1998, gives substance to and amplifies those provisions contained in the European Convention. The directive was enacted by the European Commission to permit states to bring their legislation to the same level as the minimum standards set by the EC Directive's legal framework.[79] The aim of the EC Directive is to harmonize the existing law of its member states.[80] It is the responsibility of each member state to develop its own privacy data legislation in accordance with the directive, which lays out the legal model to

---

[76] *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS 24 (1998).

[77] The term "data protection" has been highly criticized among scholars for giving the connotation that information is protected rather than individuals. *See* LLOYD, *supra* note 33, at 38.

[78] Council Directive 95/46, 1995 O.J. (L 281) 31.

[79] The justification of the EC Directive, found in Article 7(a), lies in the European Union, which aims at promoting the free movement of goods, persons, services, and capital; therefore, the EC Directive envisions that personal data should flow freely from one member State to another, but also acknowledges the necessity of safeguarding the rights of individuals in accordance with the Convention of Human Rights and Fundamental Freedoms, *supra* note 70, at art. 8. *See* Treaty Establishing the European Union, Feb. 7. 1992, O.J. (C 224/1) 448.

[80] In a remarkable case concerning the legality of a national census scheduled by the authorities, the German Constitutional court connected individuals' liberty to the processing of personal data by the intended census and ruled that if individuals do not know who is collecting the data and the purpose for such collection, the situation will eventually create an abdication of the individuals' rights to the processor's command, which cannot be tolerated in a democratic society. *See* Simitis, *supra* note 18, at 447-48 (citing Volkszahlungsurteil, 65 BVerfGE 43 (1983), *translated in* 5 HUM RTS. L.J. 94 (1984)).

follow. However, one can reasonably foresee the emergence of numerous disparities as each country enacts its own legislation, a situation that could be aggravated when different administrative agencies and courts are called on to interpret the various provisions.

The EC Directive seeks to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[81] As clearly identified by Schwarz and Reidenberg, the EC Directive has four main purposes: 1) to create norms for collecting and processing personal data;[82] 2) to provide an opportunity for affected individuals to renew information collected about themselves and to review the compiler's information practices; 3) to offer special protection for sensitive data, such as that pertaining to ethnic origins, religion, or political affiliation; and 4) to establish enforcement mechanisms and oversight systems to ensure that data protection principles are respected.[83]

The applicability of the EC Directive extends to personal data wholly or partially processed[84] by automatic and manual means, as long as they form part of, or are intended to form part of, a filing system.[85] This constitutes a major difference from its predecessor, the European Convention, which was solely intended to cover the automatic processing of information, drawing the line between manual and automatic processing. Furthermore, the EC Directive presents a two-fold exclusionary approach: 1) it is not applicable to activities that fall outside of

---

[81] EC Directive, *supra* note 78, at art. 1. It is worth mentioning that the protection of privacy rights of legal persons, such as corporations, falls outside the scope of the Directive.

[82] According to the definitions contained in the Directive, the term personal data refers to "any information relating to an identified or identifiable natural person," clarifying that an identifiable person is someone "who can be identified, directly or indirectly . . . by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity." *Id.* at art. 2, § (a).

[83] *See* Samuelson, *supra* note 41, at 763.

[84] The term "processing of personal data" is referred to as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." EC Directive, *supra* note 78, at art. 2, § (b).

[85] A filing system means "any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis." *Id.* at art. 2, § (c).

the scope of Community law, nor to matters concerning the state, such as public and national security, defense, state economic well-being, criminal investigation and breaches of ethics in the regulated professions; and 2) it is not applicable to any data related to purely personal or household activities.[86] The exclusion of the EC Directive's scope of issues, such as defense, national security, and criminal investigation, removes ambiguity for future judicial interpretations, and may clarify the application of national privacy data protection laws in a large number of cases. In contrast, American courts are often faced with the necessity of formulating judicial tests in order to confront and balance those interests.

The EC Directive undoubtedly establishes its jurisdiction by denoting that the law of each member state shall be applicable where either 1) the processing is carried out by a controller[87] in the territory of the state; or 2) the controller processes data using equipment that is located in the territory of the state. In addition, the controller has to nominate a representative for cases where he does not operate directly in the member state's territory, but uses equipment located in it.[88] Initially, the EC Directive's jurisdictional specifications pose significant consequences for the air-transport sector, particularly considering its potential extraterritorial applications. For example, bearing in mind the enormous amount of personal passenger information that carriers handle,[89] an international airline such as Aerolinas Argentinas might use an Amadeus Computer Reservation System (CRS), owned and controlled by a European carrier such as Lufthansa. Hence, even though Aerolinas Argentinas, the controller, is located outside the territorial jurisdiction of the European Union, the EC Directive will directly apply, because the

---

[86] *Id.* at art. 3. Some commentators have already expressed profound concern about the fact that sometimes it can be extremely difficult to distinguish between purely personal or household activity and the normal endeavors individuals undertake through the normal course of their labor activities. The use of a laptop, for instance, illustrates the complexity of the scenario. *See* SWIRE & LITAN, *supra* note 76, at 70.

[87] "Controller" is defined as a "natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data." EC Directive, *supra* note 78, at art. 2, § (d). From the language of the provision, it is clear that the EC Directive is applicable to both private organizations and government agencies that process personal data of individuals.

[88] *Id.* at art. 4.

[89] *See* SWIRE & LITAN, *supra* note 76, at 132.

non-European carrier is using automated equipment situated in the territory of a member state for the purpose of processing personal data.[90] One can certainly foresee that the European authorities will most likely favor the extension of such extraterritorial application to the non-European carrier when the latter handles the personal data of member states' citizens. Furthermore, the EC Directive will even be applicable to cases where a non-European airline has a frequent-flyer smart card sponsored by a European bank. The possibilities and combinations are endless, but the foregoing examples are common practices in the air-transport industry.

C. The Data Subject's Bill of Rights

The EC Directive grants a large number of privacy rights to the individual, and thus could be labelled as the "Data Subject's Bill of Rights." The individual is bestowed with the right to know both the identity of the controller and his representative, and the purposes of processing for which the data is required.[91] In other words, when an air carrier's employee swipes a passport through the reader device or inputs the data manually to comply with API procedures, he or she must inform the data subject of the purpose for which the data is collected, which in practice does not usually happen. Similarly, in more complex situations, involving, *e.g.*, smart cards with embedded biometrics, the controller must notify the data subject as to who is handling the information and for what purposes, which could be somewhat difficult to determine due to the large number of players involved. For instance, if various players were to handle passenger data on a "need-to-know" basis, tremendous difficulties could arise in simply establishing who the controller is. In an earlier article, this author observed that a state issuing machine-readable travel documents is legally obliged to inform the bearer of the details enclosed therein.[92]

As in the United States, the EC Directive grants the individual the right to access information handled by the controller. The main difference between the two previously mentioned legal regimes lies in the fact that the former only includes activities un-

---

[90] As a matter of fact, negotiations are underway between Amadeus corporate executives and the European authorities in order to reach an agreement viable for both parties. *See id.* at 133.

[91] EC Directive, *supra* note 78, at art. 10.

[92] For details of the machine-readable passport and its development in the ICAO, see Abeyratne, *supra* note 4, at 22.

dertaken by the government and its agencies, whereas the latter is particularly directed at private and public organizations that happen to store, control, or process the individual's personal data.[93] The Data Subject Bill of Rights permits the request for correction or erasure of any data processing that is not in accordance with the provisions of the EC Directive.[94] Additionally, the data subject may object to the processing of personal information at any time as long as he has legitimate grounds to do so.[95] It is important to note that the Data Subject Bill of Rights legally empowers the individual against possible invasions, intrusions, or infringements of privacy rights, whereas the burden is placed on controllers and processors of data, a situation that is totally different than in the United States.[96] Therefore, one can easily expect that privacy claims will more likely succeed within the legal spectrum of the EC Directive. In addition, the person acting under the authority of the controller or the processor must assure the confidentiality of processing, responding only to the instructions and orders of the controller, making the latter responsible in the event of any infringement of privacy rights.[97] The foregoing has direct implications for air-transport automation since almost all of the facilitation initiatives envision the inclusion of a large number of persons dealing with massive amounts of personal data.

Security concerns are also addressed by requiring those in control of databases both to provide appropriate technical and organizational measures and to avoid information leaks. Personal data protection is particularly crucial for the air-transport

---

[93] EC Directive, *supra* note 78, at art. 12, §(a). Similarly, numerous other countries, such as Argentina, Brazil, Paraguay, and Columbia concede the right to access the information the government and its agencies have on the data subject through the legal institution of the *habeas data* as a cause of action, which translated from Latin means *bring me the data.* In some countries private parties have extended the habeas data to include the processing of personal data, although the latter has created a constant doctrinal debate among scholars. It was first established in the Portuguese Constitution of 1976, and then adopted by Spain in 1978, and subsequently by a large number of countries particularly in South America. *See* JOSÉ A. MORENO RUFINELLI, NUEVAS INSTITUCIONES DE LA CONSTITUCIÓN NACIONAL 145 (1996); *see also* CONST. ARG., art. 43 (adopted 1994); CONST. PORT. art. 35 (adopted 1976); C.E. art. 18(4) (Spain) (adopted 1978); CONST. COLOM. art. 25 (adopted 1991); CONST. PARA. art. 135 (adopted 1992).

[94] EC Directive, *supra* note 78, at art. 12, §(b).

[95] *Id.* at art. 14.

[96] *See* M. P. Roch, *Filling the Void of Data Protection in the United States: Following the European Example,* 12 COMPUTER & HIGH TECH. L.J. 71, 83 (1996).

[97] EC Directive, *supra* note 78, at art. 16.

sector.[98] One of the most noteworthy achievements of the EC Directive has been the establishment of Supervisory Authorities, the bodies responsible for monitoring compliance with the Directive's provisions.[99]

The EC Directive specifically mandates that each member state provide the necessary legal remedies for any breaches of privacy rights.[100] The data subject is entitled to receive compensation from the controller in case damages are sustained. Although the burden of proof is on the controller's side, he may be exempt if he proves that he is not responsible for the damage.[101] This is the pro-"data subject" spirit of the EC Directive, which not only grants fundamental rights for the protection of privacy but also provides the mechanisms to correct any deviation in the system. Perhaps this is one of the advantages of creating a specific legal framework to deal with an emerging problem or, where every situation has been carefully studied, of trying to envision all possible derivatives— as opposed to the U.S. approach of letting the existing legal system respond to each rising difficulty and develop from experience. However, the detractors of the EC Directive would argue that its legal framework is rather static and inflexible, handicaps that do not allow the judiciary to adapt themselves quickly enough to emerging technological advancements. Under the U.S. approach, judicial innovation will always precede the enactment of legal rules, and the entrepreneurial air-transport sector will not be in favor of adopting a stationary business attitude requiring them to await legal regulations to solve newly arising problems.

The EC Directive asserts that member states, through the application of their national laws, must guarantee the Directive's full implementation and must impose sanctions in the case of violations.[102] This obligation placed on member states repre-

---

[98] *Id.* at art. 17.

[99] *Id.* at art. 18, § (1). For instance, the controller or his representative must inform the Supervisory Authority before carrying out any automatic processing of personal data. In the air transport context, this means that each incumbent in the business must first identify who is the controller of the personal data, and notify the supervisory authority in its respective country. The contents of the notification should include the name and address of the controller and of his representative, the purpose of processing, a description of the categories of the data relating to the data subject, the recipient of the categories, and any proposed transfers of data to third countries. *Id.* at art. 19.

[100] *Id.* at art. 22.

[101] *Id.* at art. 23.

[102] EC Directive, *supra* note 78, at art. 24.

sents a risk for controllers, who will be forced to demand that insurers extend insurance coverage against any possible liability that might arise, thereby swelling premium rates and operational costs.[103]

III. PRIVACY ISSUES IN CANADA

Canada, although not as prolific in its legislation as the United States and Europe, nonetheless remains a significant player in automation. Canada has drawn on both approaches of the United States and Europe in the protection of privacy rights.[104] The latest trends in Canadian regulation of privacy data protection, although balancing both conflicting interests, reflect a *suis generis* model.

As in the United States, the dichotomy of the two-fold approach between the public and private dimensions also appears in the Canadian context. The Canadian Charter of Rights and Freedoms encompasses the public sphere of privacy data protection, addressing the relationship between individuals and the government.[105] Canadian courts have determined that two particular sections of this Act indirectly address privacy issues. Section 7 provides that "everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice,"[106] and Section 8 is the equivalent of the Fourth Amendment to the U.S. Constitution, protecting individuals against unreasonable search and seizure.[107]

In the 1984 case *Hunter v. Southam Inc.*,[108] involving the unreasonable search and seizure provision of Section 8 of the Canadian Charter, the Supreme Court of Canada acknowledged the existence of the right of privacy as the right to be let alone. The Court found that the right of privacy "is the right to be secure against encroachment upon the citizens' reasonable expectation

---

[103] *See* HANDBOOK ON COST EFFECTIVE COMPLIANCE WITH DIRECTIVE 95/46/EC 78, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/studies/handbook.pdf.

[104] *See generally* DAVID H. FLAHERTY, PROTECTING PRIVACY IN TWO-WAY ELECTRONIC SERVICE 11 (1985).

[105] CAN. CONST. (Constitution Act, 1982), part I (Charter of Rights and Freedoms), ch. 11, § 7.

[106] *Id.*

[107] *Id.* § 8.

[108] [1984] 2 S.C.R. 145.

of privacy in a free and democratic society."[109] In its decision, the Court favored a case-by-case analysis to determine whether the law gives a remedy for the invasion of privacy.[110] The Court interpreted privacy similarly to the United States, examining the individual's "reasonable expectation of privacy." Therefore, one can reasonably say that when a case involves privacy infringement by federal government agencies as a result of implementing automation endeavours in air transport, Canadian courts, like their U.S. counterparts, may tend to apply the reasonable expectation of privacy test. In addition, Canada has enacted the *Privacy Data Act*,[111] governing the collection, use and disclosure of personal information and regulating the conduct of federal agencies with respect to the processing of such data, and the *Access to Information Act*,[112] granting individuals access thereto. Numerous Canadian provinces have also adopted privacy legislation.[113] Both the federal government and the provinces can exercise jurisdiction on privacy matters. The most significant fact, particularly at the provincial level, stems from the fact that Canada has extended the jurisdiction of the Privacy Commission to include not only the provisions dictated by the *Privacy Act*, but also to those of the *Freedom of Information Act*.[114] This watchdog institution plays a significant role in the protection, investigation, enforcement, and mediation of privacy rights in Canada at the provincial and federal level.

A. THE EMERGENCE OF A SUI GENERIS MODEL

Canadians have hitherto not had a single comprehensive legislation with respect to the private sphere of privacy data protection, but, rather, sectoral regulation attempting to address

---

[109] *Id.* at 159 (quoting Southam, Inc. v. Dir. of Investigation & Research, [1983] 24 Alta. L.R.2d 307).

[110] Similar decisions in Canadian courts were reached in *Scanne v. Orr*, [1981] 34 O.R.2d 317 (Co. Ct.) and *Lipiec v. Borsa* [1996], 31 C.C.L.T. (2d) 294 (Ont. Gen. Div.). The right of privacy has been protected in Canada and the Commonwealth countries under a myriad of different legal theories, *inter alia*, contract, trespass, nuisance, and defamation. *See* Green v. Minnes, [1891] 22 O.R. 177 (C.A.); Motherwell v. Motherwell, [1976] 73 D.L.R. (3d) 62 (Alta. C.A.); Robbins v. C.B.C., [1957] 12 D.L.R.2d 35.

[111] Privacy Act, R.S.C., ch. P-21 (1985).

[112] Freedom of Information Act, R.S.C., ch. A-1 (1985).

[113] *See* Privacy Act, R.S.B.C., ch. 373 (1996) (B.C., Can.); Privacy Act, R.S.M., ch. P125 (1987) (Man., Can.); Privacy Act, Nfld. R.S., ch. P-22 (1990) (Nfld., Can.); Privacy Act, S.S., ch. P-24 (1978) (Sask., Can.).

[114] *See* David H. Flaherty, *Some Reflections on Privacy and Technology*, 26 MAN. L.J. 219, 222 (1999).

specific privacy issues related to certain industries.[115] Had the privacy issue not been contemplated by one of the sectoral legislations enacted, the matter would have been resolved by the tort of privacy in the common law provinces, and by statute in the civil law Quebec.[116] The tort of privacy invasion has faced the same difficulties and shortcomings as the one contained in the United States system. Quebec, following the European example, has adopted the *Act Respecting the Protection of Personal Information in the Private Sector*,[117] which extended the application of privacy data protection to the processing performed by government agencies, as well as private parties, constituting an innovation in North America.[118] This act regulates the collection, use, and disclosure of personal information held by the private entrepreneurial sector operating in Quebec, and grants the individual the right of access to such information. Moreover, Quebec's Civil Code grants the protection and respect of privacy rights.[119] Thus, the legal framework established in Quebec would seem to be the only one that is in accord with the stringent requirements contained in the EC Directive. Some commentators have suggested that the level of privacy protection in Canada offered at the provincial level considerably exceeds that of the federal government with respect to the private sector.[120]

---

[115] *See e.g.* Telecommunications Act, R.S.C., ch. T-3.4, §§ 39,41 (1993) (Can.); Bank Act, R.S.C., ch. B-101, §§ 242, 244, 259 (1991) (Can.); Insurance Companies Act, R.S.C., ch. I-11.8, §§ 489, 607 (1991) (Can.); Trust and Loan Companies Act, R.S.C., ch. T-19.8, §444 (1991); Canada Pension Plan Act, R.S.C., ch. C-8, § 104 (1985).

[116] For a comprehensive study on Canadian common law torts, see John D. R. Craig, *Invasion of Privacy and Charter Values: The Common-Law Tort Awakens*, 42 McGILL L.J. 355 (1997). For Quebec civil law privacy data protection, see KARIM BENYEKHLEF, LA PROTECTION DE LA VIE PRIVÉE DANS LES ÉCHANGES INTERNATIONAUX D'INFORMATIONS 92 (1992); Paul-Andre Comeau & Andre Ouimet, *Freedom of Information and Privacy: Quebec's Innovative Role in North America*, 80 IOWA L. REV. 651 (1995); H. Patrick Glenn, *The Right to Privacy in Quebec Law*, *in* ASPECTS OF PRIVACY LAW 41(Dale Gibson ed., 1980); René Laperrière, *The 'Quebec Model' of Data Protection: A Compromise between Laissez-faire and Public Control in a Technological Era*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 182 (Colin J. Bennett & Rebecca Grant eds., 1997).

[117] S.Q., ch. 17 (1993).

[118] *See* Comeau & Ouimet, *supra* note 116, at 651.

[119] *See* C.C.Q., arts. 35-41 (1993) (Can.).

[120] *See* COLIN J. BENNETT, IMPLEMENTING PRIVACY CODES OF PRACTICE 8 (1995).

B. The Personal Information Protection and Electronic Documents Act

In order to balance the disproportion created by the *Act Respecting the Protection of Personal Information in the Private Sector* enacted in Quebec with respect to the other provinces, and the fragmented federal regulation (or the lack thereof), Canada has enacted federal legislation. After a long process of negotiations, an agreement was reached in the *Personal Information Protection and Electronic Documents Act*,[121] which was passed on April 13, 2000. The Act came into force progressively on January 1, 2001, and comprises two main parts: 1) the protection of personal information, and 2) the regulation of electronic documents as an alternative to the use of paper to record information or transactions.[122] The Act seeks to establish rules governing "the collection, use, and disclosure of personal information" in a manner that balances the right of privacy of all individuals with "the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[123] The foregoing represents a credible attempt to consider not only the interests of the individual in protecting his privacy rights, but also a remarkable effort not to place an enormous burden on the private entrepreneurial sector. It represents an approach that favors the adoption of privacy data protection legislation without hindering the normal course of private business. The Act was passed only after consideration of market implications on the private sector. It is the result of a consensus reached among the many players involved. The Act was based on the Canadian Standards Association's *Model Code for the Protection of Personal Information.*[124] The latter has been included in the Act as "Sched-

---

[121] S.C., 5 (2000).

[122] *Id.* §§ 3, 32.

[123] *Id.* § 3; *see also Backgrounder: Privacy Provisions Highlights, available at* http://e-com.ic.gc.ca/english/fastfacts/43d8.html (last visited July 28, 2000). Personal information is defined in the act as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. Personal Information Protection and Electronic Documents Act, S.C. ch. 5, at § 2(1). However, the act does not apply to personal information used, collected, or disclosed by an individual for a personal purpose, or by an organization for journalistic, artistic, literary, or any activity outside of its commercial purpose. *Id.* § 4.

[124] The Canadian Standards Association has established ten principles for a Model Code for the Protection of Personal Data, including: 1) *Accountability Principle,* making the organization responsible for personal information under its

ule 1", aiming at providing the private entrepreneur with guidelines, principles, and suggestions for the development of adequate mechanisms in order to properly safeguard individuals' personal information.[125] Herein lies one of the main differences between the Canadian law and the EC Directive: the EC Directive was enacted more out of favoritism for the individual's right of privacy, conceived as a fundamental human right, rather than as a balance between competing interests between individuals and private entrepreneurs, as in the Canadian context.

The Canadian act was designed to be implemented in three different phases: 1) for organizations in the federally regulated private sector, such as airlines, telecommunications, banking, broadcasting, and interprovincial transportation, beginning January 1, 2001, 2) for health information, beginning January 1, 2002, and 3) for full application, including commercial use of personal information, whether or not regulated by federal law, on January, 1 2004.[126] The rationale behind this progressive implementation of the Act lies in the fact that certain industry sectors might require more time to adapt to the new privacy data requirements. Needless to say, the Act's first phase of imple-

---

control; 2) *Identifying Purposes Principle*, whereby the intention behind the collection of such data must be identified to the data subject at or before the information is collected; 3) *Consent Principle*, making consent and knowledge necessary for the collection, use or disclosure of personal information; 4) *Limiting Use, Disclosure, and Retention Principle*, whereby personal information shall only be used for its intended purpose, disclosed with the individual's consent, and retained only for the necessary time to comply with its objective, unless otherwise required by the laws; 5) *Limiting Use, Disclosure, and Retention Principle*, whereby personal information shall only be used for its intended purpose, disclosed with the individual's consent, and retained only for the period of time necessary to comply with its objective, unless otherwise required by law; 6) *Accuracy Principle*, meaning that personal information must be precise, complete and up-to-date; 7) *Security Principle*, whereby personal information shall be protected from unwanted intrusion; 8) *Openness Principle*, whereby the organization makes available to the individual, information about its policies and practices with respect to the handling of personal information; 9) *Individual Access Principle*, whereby an individual is granted access to the organization's record of his personal information upon request; and 10) *Challenge and Compliance Principle*, whereby an individual is capable of challenging the agency's compliance with the aforesaid principles to a specific institution. *Id.* at schedule 1. *See also Canadian Standards Ass'n, Model Code for the Protection of Personal Information, available at* http://www.csa-international.org/english/product_services/ps_privacy.html (last visited July 30, 2000).

[125] Personal Information Protection and Electronic Documents Act, at sch. 1.

[126] Privacy Commissioner of Canada, Personal Information Protection and Electronic Documents Act—Implementation Schedule, *at* http://www.privcom.gc.ca/legislation/index_e.asp (last visited July 29, 2000).

mentation will already affect air carriers' common practices and operations, which could have significant consequences on implementing automation initiatives in air transport. One can easily envision that the air-transport players might have to redesign numerous practices and procedures in order to comply with the Act's requirements.

C. The "Reasonable Collection, Usage and Disclosure" Principle

The Act denotes that an organization may collect, use, or disclose personal information solely for "purposes that a reasonable person would consider are appropriate in the circumstances,"[127] incorporating the longstanding common-law rule of reasonableness. It will depend on the Privacy Commissioner and the courts to interpret the legal parameters of reasonable purposes in appropriate circumstances. The language of the Act suggests a slightly different connotation than the one contained in the EC Directive, which makes reference to the collection of data for "specified, explicit and legitimate purposes."[128] The latter has a smaller discretionary spectrum, whereas the former enlarges the Act's interpretive power.

1. The "Consent and Knowledge" Principle

The Act follows the European principle of data protection, namely that the information cannot be collected or used without the consent of the data subject; however, the Canadian legislation extends the latter to include the individual's consent and knowledge thereto.[129] The purpose of this extension is to ensure that private organizations make all necessary efforts to reasonably let the data subject know and understand how the information will be handled. This means that organizations wishing to implement automation initiatives must clearly obtain the consent of the data subject and at the same time inform him of the intention of the processing and usage thereof. Nevertheless, the Act provides exceptions where data can be processed without the data subject's consent; for example, where the collection is clearly in the interests of the individual, where the in-

---

[127] Personal Information Protection and Electronic Documents Act, S.C. ch. 5, § 5(3).

[128] *Compare id.* § 5(3) *with* EC Directive, *supra* note 78, at art. 6(b).

[129] *See* Personal Information Protection and Electronic Documents Act, S.C. ch. 5, sch. 1, § 4.3.2.

formation is already publicly available, or where the organization has reasonable grounds to believe that the individual might be contravening Canadian laws.[130]

Canadian legislation provides that organizations cannot use an individual's personal information without the knowledge or consent of the data subject, unless otherwise required by law.[131] The data subject can request, in writing, individual access to the information,[132] and the organization must respond within thirty days of receiving this request.[133] However, organizations can extend the period for another thirty days, where the request "unreasonably interferes with the activities of the organization," or where more time is required to convert the data subject's information into an alternative format.[134] The Act also provides remedies where an individual's right of privacy is violated, in which case the data subject may file a written complaint with the Privacy Commissioner,[135] and, once a report has been issued on the matter, may apply to the courts for a hearing.[136] One can easily expect that the preceding requirements will somewhat change the industry players' procedures and practices.

2. *Transborder Data Flows*

On its face, the Act does not present any significant legal barrier to the transborder flow of personal data, although it mandates that where personal information is transferred for processing to a third party, organizations must enter into a contractual relationship with such party to ensure a sufficient level of privacy protection.[137] This presents a more flexible requirement than the adequacy principle envisioned within the European legal framework, which establishes that personal

---

[130] *Id.* § 7(1).

[131] *Id.* § 7(2).

[132] *Id.* § 8(1); *see also id.* at sch. 1, § 4.9.

[133] *Id.* § 8(3).

[134] Personal Information Protection and Electronic Documents Act, S.C. ch. 5, § 8(4).

[135] *Id.* § 11. The Commissioner may even conduct audits of the practices of certain organizations where he has reasonable grounds to believe that such enterprise may be contravening the provisions of the act. *Id.* at § 18(1). Similarly, the act contains a whistle blowing provision, whereby any person who has reasonable grounds to believe that a person or an organization has infringed the act may notify the Commissioner. *Id.* § 27.

[136] *Id.* § 14. The court could order the organization to correct its practices and procedures, or even award damages to the plaintiff. *Id.* § 16.

[137] *Id.* sch. 1, § 4.1.3.

information can only be transferred to third countries that offer the same standard or level of privacy protection. Although exceptions are provided, this represents the general rule, while the Canadian Act provides an alternative mechanism, such as the adoption of contractual provisions by the parties, instead of directly restricting the flow of personal data as done by the EC Directive.

The spirit of the Act calls for the avoidance of possible legal hurdles facing the entrepreneurial sector, providing for the long-awaited combination of legal regulation and business self-participation. The private sector's initiatives, which are carefully observed by government authorities from an "arm's-length" distance, become of paramount importance in the proper development of the system. One can certainly envision a large number of contractual provisions governing the relationships of diverse players when implementing automation initiatives in air transport. For example, Air Canada may be particularly keen on drafting thorough contractual provisions to govern its contractual relationships with those enterprises that handle the personal information of its passengers' frequent flyer smart cards, as in the case of banking institutions. Another relevant provision of the Act refers to the safeguards necessary to guarantee the security of personal information. It establishes that organizations should include: 1) physical measures, such as restricting access to the organization's offices; 2) organizational measures restricting access to sensitive information according to the "need to know" principle; and 3) technological measures favoring the use of passwords and encryption.[138] These principles certainly apply to all the automation endeavors envisioned in this article, and could represent a valuable tool to avoid any information leaks in the system. As previously explained, such leaks could have awful consequences for individuals' right of privacy, especially when one considers the large amounts of data involved.

Although by no means a comprehensive legal remedy for problems posed by the privacy issues inherent in data storage and the exchange of information, the Canadian Act represents a novel approach to the issue of privacy data protection, primarily because it was created through a consensus of regulators, industry players and privacy organization groups. Privacy data protection in Canada is certainly consistent with the stringent

---

[138] *Id.* at sch. 1, § 4.7.3.

standards established by European legislation, particularly with the recent enactment of the *Personal Information Protection and Electronic Documents Act* in accordance with the EC Directive's strict requirements. Consequently, issues of transborder data flows are most likely not to occur between the two parties. However, the Act strongly encourages the adoption of alternative mechanisms by means of contractual provisions, as well as the implementation of the long-awaited Model Code on Data Protection.

IV. CONCLUSION

Individuals have a legal right to know what goes into a data bank with regard to their own details. Accordingly, states that store such information are legally obligated to inform individuals of the nature of the details that might be included in public documents, such as their passports. Likewise, states should make arrangements to inform individuals of the information stored in governmental computers relating to them. Any indecipherable data should be clearly explained to the individual so that he can: 1) determine whether such data should be disclosed to the public; 2) determine the accuracy of the details entered into the computer; 3) be informed of the specific use of his personal data that is stored in the computer; 4) be informed of the type of persons who would have access to the personal data that is stored; and 5) evaluate the amount of personal information about him that is actually stored.

Since the data contained in such documents, such as passports and visas, are machine readable and would be subject to transborder storage, there is a compelling need to consider the introduction of uniform privacy laws so that the interests of the data subject and the data seeker are protected. Although complete uniformity in privacy legislation may be a difficult objective to attain,[139] it will be well worth the while of the international community to at least formulate international standards and recommend practices, along the lines of the various ICAO Annexes, to serve as guidelines for state conduct. After all, as Collin Mellors pointed out: "Under international agreements . . . privacy is now well established as a universal, natural, moral and human right." Article 12 of the Universal

---

[139] *See* Gordon C. Everest, *Nonuniform Privacy Laws: Implications and Attempts at Uniformity, in* COMPUTERS AND PRIVACY IN THE NEXT DECADE 146 (Lance J. Hoffman ed., 1980).

Declaration of Human Rights, Article 17 of the United Nations Covenant on Civil and Political Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms all specify this basic right to privacy. Man everywhere has occasion to seek temporary "seclusion or withdrawal from society" and such arrangements cannot define the precise area of the right to privacy.[140] Such a definition is needed to reconcile the interests of ensuring respect for individuals' information and privacy on the one hand and the encouragement of free and open dissemination of transborder data flows on the other.

As for the use of biometric information such as hand geometry and eye scanning, such purely biological information should be used only for identification purposes with explicit assurances by the authorities that the information will not be used for any other purpose. Before a process for the collection of such information is formally put into practice, legal issues of ownership and patent should be carefully thought out, and given the utmost consideration.

---

[140] Collin Mellors, *Governments and the Individual—Their Secrecy and His Privacy, in* PRIVACY 94 (John B.Young ed., 1978).


SOUTHERN METHODIST UNIVERSITY
DALLAS, TEXAS