Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard

BARTOSZ M. MARCINKOWSKI*

TABLE OF CONTENTS

I. INTRODUCTION

In this Article, I will examine a phenomenon that I refer to as the privacy paradox (or paradoxes, as I identify several of them). This phenomenon appears in the Euro-Atlantic discussion on privacy and personal data protection.

---

* Partner at Domański Zakrzewski Palinka (DZP) law firm in Warsaw, Poland; PhD student at the Cardinal Stefan Wyszyński University (UKSW) in Warsaw. The author wishes to thank his doctoral thesis supervisor, Professor Irena Lipowicz, head of the Polish Ombudsman office; Krzysztof A. Zakrzewski, Managing Partner at DZP, and Professor Peter P. Swire, the Nancy J. & Lawrence P. Huang Professor at the Georgia Institute of Technology, for their support, encouragement, and the opportunity to present his views.

> The Poles, more than any other nation [had the misfortune of experiencing] the most audacious and complex versions of obsessions with projects of a perfect society—the one-thousand-year Third Reich and the gardens of Eden of communism . . . [The Poles know] what it is like to live in a society-garden, with state as gardener.[1]

As a Pole, I feel inclined to take part in discussion on the issue at hand.

There is another reason why the analysis of the European and American personal data protection systems carried out from the perspective of a Polish researcher is particularly attractive. And that is the fact that the Polish Personal Data Protection Act of 1997[2] is virtually a word-for-word transposition of the EU Data Protection Directive of 1995.[3] Hence the Polish regulation reveals and puts to a test the intentions of the EU legislator.

My aim is to follow the principles of comparative legal doctrine in an attempt to avoid falling into the EU- or U.S.-centrism trap.

As mentioned, this Article will focus on comparative research from the perspective of a European legal practitioner with close to twenty years of professional experience in Poland—an EU member state and a vital European and global center for business support services, which entails intensive data transfers to and from Poland.

In my Paper I will (i) introduce the issue at hand, (ii) define basic terminology, (iii) discuss the axiological basis of the European and American regulations, (iv) describe systemic differences between them, (v) present evolutionary tendencies of both legal systems, and (vi) outline a proposed method of convergence.

II. THE TRANSATLANTIC DEBATE

The axis of the argument prevailing in the EU is that the American legal system does not ensure an adequate (from EU legal perspective) degree of personal data protection, which results in significant limitations to transfers of data from the European Union (including Poland) to the United States. I therefore adopt, as a working hypothesis, a widely held stance that European regulations, particularly the EU Data Protection Directive, are the point of reference for comparisons and analyses. In practice, this assumption results in promoting the European standards as a benchmark for assessing the effectiveness of other, non-European informational privacy systems. At the same time, the test of adequacy of data protection in non-European countries is

---

[1] ZYGMUNT BAUMAN, CIAŁO I PRZEMOC W OBLICZU PONOWOCZESNOŚCI [BODY AND VIOLENCE IN THE FACE OF POSTMODERNITY] 21 (1995) (translation provided by author).

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [Polish Data Protection Act of 1997] (1997 r. Dz.U. Nr 133, poz. 883 as amended).

[3] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter EU Data Protection Directive] (on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

complex, contextual, and holistic, referring to the circumstances of data processing in its entirety.[4] Such nature of the tests results in a lack of uniformity of the criteria applied and an unclear hierarchy thereof.

The above observations do not imply that the said principles and minimum data security requirements established by the EU legislator constitute an absolute and indisputable global standard for personal data protection. At the same time, however, as noted correctly by Colin J. Bennett and Charles D. Raab, European personal data protection standards are exported from Europe to other parts of the world, including the United States (which from the perspective of other civilizational phenomena is not a typical or obvious direction).[5] We can therefore talk about the California Effect à rebours.[6] Nevertheless, both the European Union and the United States clearly express their determination to map out the ultimate global standard on privacy and personal data protection, each of them in accordance with their own conceptual model.[7] Both actors in the Transatlantic debate (i.e. the EU and the United States) adopt a stance that their respective data protection instruments—that is, a precise, explicit, and specific public-law regulation in Europe, and flexible, pro-market, based on self-regulating free-market principles, segmented, sector regulation in the United States—should prevail.[8]

A. *The Significance of the Issue*

There are no doubts over the significance of the issue of privacy (informational privacy) protection in today's world dominated by the Internet and phenomena such as Big Data and Open Source.[9] Personal data has become

---

[4] *Id.* arts. 25–26, at 45–46; 1997 r. Dz.U. Nr 133, poz. 883 as amended. *See generally* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV D/5025/98, WP 12 (July 24, 1998), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

[5] COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 114 (2006).

[6] SEBASTIAAN PRINCEN, EU REGULATION AND TRANSATLANTIC TRADE 5–6 (2002).

[7] European Council, The Stockholm Programme—An Open and Secure Europe Serving and Protecting Citizens, 2010 O.J. (C 115) 1, 11; THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 31–33 (2012) [hereinafter CONSUMER DATA PRIVACY], *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; *see also* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 21 (1998).

[8] *See* Priscilla M. Regan, *American Business and the European Data Protection Directive: Lobbying Strategies and Tactics*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 199, 212 (Colin J. Bennett & Rebecca Grant eds., 1999).

[9] *See* Case C-138/11, Compass-Datenbank GmbH v. Republik Österreich, 2011 EUR-Lex CELEX LEXIS 0138 (July 12, 2012), *available at* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=req&doci

a tangible asset in such a world. As noted by Alan F. Westin, privacy—including personal data—some fifty years ago constituted a "third-tier social, political, and legal issue."[10] Nowadays, civilizational advances are linked to information processing, hence privacy and personal data protection have become paramount issues in the world governed and driven by modern technologies.[11]

At the beginning of the twenty-first century, the value of trade between the EU and United States was estimated at some USD 120 billion at both ends.[12] According to the EU Digital Agenda, paradoxically "Europeans often find it easier to conduct a cross-border [Internet] transaction with U.S. business than with one from another European country,"[13] while data on EU consumer behavior and preferences have been available in the United States for years.[14] Still, according to a widely held belief in Europe, personal data is not adequately protected in the United States.

Nonetheless, limiting the issue of informational privacy protection to a *strict* commercial sphere, in my opinion, oversimplifies and trivializes the issue. I believe that the issue of informational privacy, in a way, determines the degree

---

d=124999&occ=first&dir=&cid=6123250; TERENCE CRAIG & MARY E. LUDLOFF, PRIVACY AND BIG DATA 4 (2011); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 2 (2013); Christopher Kuner et al., *The Challenge of "Big Data" for Data Protection*, 2 INT'L DATA PRIVACY L., May 2012, 47, 47–48 (2012); Bartosz Marcinkowski & Sylwia Kuca, *Incydent czy znak czasu?* [*An Incident or a Sign of the Times?*], RZECZPOSPOLITA PRAWO (Mar. 14, 2013, 11:07 AM), http://prawo.rp.pl/artykul/989792.html (translation provided by author); *Compliance News Updates*, PDP (Mar. 19, 2013), http://www.pdpemail.com/compliance 19032013/.

[10] Alan F. Westin, *How Important Is Privacy Today?*, IAPP (Dec. 17, 2012), https://www.privacyassociation.org/publications/2012_12_17_how_important_is_privacy_today.

[11] *See* Daniel J. Solove, *A Brief History on Information Privacy Law*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 1:1 (Kristen J. Matthews ed., 2006); Marek Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym* [*The Right to Privacy and Personal Data Protection in an Information Society*] 6 PAŃSTWO I PRAWO 3 (2002) (translation provided by author); Westin, *supra* note 10.

[12] Lee A. Bygrave, *International Agreements To Protect Personal Data*, *in* GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION 15, 15 (James B. Rule & Graham Greenleaf eds., 2008) (citing DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 2 (2005)); *see also* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 179 (1999); Stephen J. Kobrin, The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance 24 n.18 (Nov. 2002) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=349561.

[13] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, at 10, COM (2010) 245 final/2 (May 19, 2010).

[14] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 308 (1996).

of personal freedom of an individual and has a direct influence on the foundations of a democratic civil society.

Threats to and the abuse of personal data (informational privacy) may come from different directions—not only from authorities,[15] but also business entities. It is estimated that Google performs and maintains in its archives some three billion search queries every day; thus the data stored by Google every day has by now become a limitless source of information about Internet users.[16] This data can be used in a variety of ways in different political and social conditions in order to influence individuals.

One may of course argue that the issue of personal data protection is an intellectual exercise for developed and affluent Western societies, while limitations to or complete loss of informational privacy is an inevitable cost of innovation and development of a society. In my view, however, such underestimation of the issue is improper, as it undermines the basic values that are fundamental to a free and democratic society (this issue will be discussed more in the latter part of this Article). Rapidly advancing technological revolution is, paraphrasing Abraham Maslow, a catalyst of changes, from which a new image of the human being, society, science, basic values, and philosophy emerge, while privacy—including informational privacy in particular—is located among basic needs, which are part of a wider need of safety (that are placed just above basic physiological needs).[17]

B. *Terminology*

Further deliberations on the topic require some clarification and systemization of the terminology used in the Euro-Atlantic debate, insofar as the limitations of this Article allow. Apart from basic systemic differences between the system of statutory law (European) and the system of common law (United States) (more on this issue in the latter part of this Article), the linguistic layer constitutes an additional barrier and a common source of misconceptions or misunderstandings. Further clarification is also needed in order to avoid the problem of comparing notions that represent values that belong to different categories.[18]

---

[15] An interesting case in point surfaced in the summer of 2013 when details about PRISM—an NSA security intelligence and surveillance program, which collects data from the systems of some of the biggest tech companies—were revealed. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; *see* A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965, 991–94 (2013).

[16] MAYER-SCHÖNBERGER & CUKIER, *supra* note 9.

[17] ABRAHAM H. MASLOW, MOTIVATION AND PERSONALITY 18–20, 67–72 (3d ed. 1987).

[18] ROMAN TOKARCZYK, KOMPARATYSTYKA PRAWNICZA [COMPARATIVE LEGAL STUDIES] 34 (2008) (translation provided by author).

Up to this point I have used terms such as "personal data" and "informational privacy." Meanwhile, the EU legislation and that of its member states provides a precise definition of "personal data," that is: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[19] This definition is, in principle, identical to the one that appears in the Polish Personal Data Protection Act (Article 6).[20] In addition, this definition conforms with the definition set out in Article 4(1) of the draft General Data Protection Regulation,[21] which, according to a proposed reform of the EU legal system,[22] is intended to replace the EU Data Protection Directive, and European national regulations.[23]

In the American literature the notion of "personal data" appears in different contexts with different intensity. For instance, a definition similar to the European definition is used by the authors of a government document, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*.[24] In this document, personal data is defined as any information, including aggregated information (connected to other information) that is linkable to a specific individual, including by a computer or a telephone that can be used to profile a person, even when such a computer or a telephone is not used exclusively by one individual.[25] Prior to that, similar definitions appeared also at the working stage on the federal Privacy Act of 1974, during which the notion of "personal information" was used to mean:

> [A]ny information about the individual that identifies or describes any characteristic including but not limited to education, financial transactions, medical history, criminal or employment record, or any personal information

---

[19] EU Data Protection Directive, *supra* note 3, art. 2(a), at 38.

[20] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [Polish Data Protection Act of 1997] (1997 r. Dz.U. Nr 133, poz. 883 as amended).

[21] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 41, COM (2012) 11 final (Jan. 25, 2012).

[22] *Id.*

[23] A *directive* needs to be implemented in each EU member state, allowing each national legislator to adopt their own measures in order to achieve the intended result. A *regulation* becomes part of all national legislations, ensuring full uniformity of legal norms across all EU member states. KLAUS-DIETER BORCHARDT, THE ABC OF EUROPEAN UNION LAW 88–89 (2010).

[24] CONSUMER DATA PRIVACY, *supra* note 7, at 10.

[25] *Id.* at 10 n.12. Sometimes the expression "personally identifiable information" (PII) is used in government documents, in a sense that in principle is identical to the definition above. *Id.*

> that affords a basis for inferring personal characteristics such as finger and voice prints, photographs, or things done by or to such individual. Such definition includes the record or present registration, or membership in an organization or activity, or admission to an institution. It is intended to include within these terms any symbol, number, such as a social security number or character, address, by which the individual is indexed in a file or retrievable from it.[26]

The above does not change the fact that a central notion connected with the field labeled in Europe as "personal data protection" is denominated as "privacy" in the United States.[27]

The notion of "privacy" is, however, significantly wider in its scope than the notion of "personal data," which becomes apparent as dozens of "privacy" subcategories emerge in literature on the subject.[28] Among the most important I would include "decisional privacy,"[29] "physical privacy" (also referred to as "spatial"/"territorial privacy"),[30] as well as "informational privacy," which I will discuss in more detail, below.

The decoding of "privacy" is subjective and dependent on complex social, cultural, historical, and even geographical factors,[31] although some scholars believe that there is an internal "value order" that would indicate which areas of privacy should remain unconditionally sacred and inviolable.[32] Nevertheless, it

---

[26] S. REP. NO. 93-1183, at 78–79 (1974).

[27] What is referred to in Europe as "personal data protection," in American literature is often linked with intellectual property rights or security measures in IT systems. SCHWARTZ & REIDENBERG, *supra* note 14, at 5–6.

[28] A Polish researcher, Krzysztof Motyka, identified over 120 subcategories of "privacy" in American literature, classified according to a variety of different criteria. Krzysztof Motyka, *Prawo do prywatności* [*The Right to Privacy*], *in* 2 ZESZYTY NAUKOWE AKADEMII PODLASKIEJ W SIEDLCACH 9, 25–34 (2010) (Pol.) (translation provided by author).

[29] William A. Edmundson, *Privacy*, *in* THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 271, 272–73 (Martin P. Golding & William A. Edmundson eds., 2005); *see also* Roe v. Wade, 410 U.S. 113, 129 (1973).

[30] *See* PETER P. SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS AND PRACTICES 2 (Terry McQuay ed., 2012).

[31] *See* CRAIG & LUDLOFF, *supra* note 9, at 15; MASLOW, *supra* note 17, at 212–13 (on changing social conventions and their cultural and geographical variations); WITOLD RYBCZYNSKI, HOME: A SHORT HISTORY OF AN IDEA 28 (1986); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155, 1159 (2004).

[32] *See* Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 759 (1989); *see also* MARC ANCEL, ZNACZENIE I METODY PRAWA PORÓWNAWCZEGO [THE IMPORTANCE AND METHODS OF COMPARATIVE LAW] 32–33 (1979) (translation provided by author); Marek Safjan, *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych* [*Reflections on Constitutional Determinants for the Development of Personal Data Protection*], *in* XI KWARTALNIK PRAWA PRYWATNEGO 223, 243 (2002) (translation provided by author); Mikołaj Wild, *Ochrona prywatności w prawie cywilnym* [*Privacy Protection in*

is impossible to indicate the sacred and inviolable boundary of privacy in an *a priori* defined set of circumstances.[33] Hence the conclusion that the notion of privacy remains difficult to define.[34]

Even more so, it is necessary to extract a subcategory of privacy in accordance with its usage in the United States in order to be able to compare it with the European notion of personal data protection. To this end, a subcategory of "personal privacy" seems appropriate. It appears, among other sources, in the American *Records, Computers and the Rights of Citizens* report of the Secretary's Advisory Committee on Automated Personal Data Systems, drawn up for the Department of Health, Education, and Welfare in 1973.[35] The report defines "personal privacy" as the right of individuals and/or organizations to decide which information about them may be transferred to other parties.[36] However, in the American literature, the notion used most often with reference to the protection of information with regard to individuals (personal data protection) is "informational privacy,"[37] which comes down to "control over personal information"[38] (hence it is often referred to as "disclosural privacy," which in my opinion narrows it down excessively)[39] and "privacy" with regard to "personal information."[40] From this perspective, a definition proposed by Alan F. Westin, referring to the right of individuals to control, edit, manage, and delete information about themselves and decide when, how, and to what extent information is communicated to others seems quite appropriate.[41]

Taking into consideration the above, further deliberations should refer to legal mechanisms used for "personal data protection" in the European Union,

---

Civil Law] *(Koncepcja sfer a prawo podmiotowe)*, *in* 4 PAŃSTWO I PRAWO 54, 56 (2001) (translation provided by author).

[33] Wild, *supra* note 32, at 66.

[34] MARIUSZ JAGIELSKI, PRAWO DO OCHRONY DANYCH OSOBOWYCH: STANDARDY EUROPEJSKIE [THE RIGHT TO PERSONAL DATA PROTECTION: EUROPEAN STANDARDS] 22–23 (2010) (translation provided by author); Whitman, *supra* note 31, at 1153.

[35] SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 40–41 (1973) [hereinafter HEW REPORT].

[36] *See id.*

[37] Edmundson, *supra* note 29, at 272.

[38] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION AND TECHNOLOGY 44–45 (2d ed. 2009); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1109 (2002); *see also* SWIRE & AHMAD, *supra* note 30, at 2.

[39] *See* Todd Robert Coles, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 962–63 (1991); Timothy O. Lenz, *"Rights Talk" About Privacy in State Courts*, 60 ALB. L. REV. 1613, 1624 (1997); Motyka, *supra* note 28, at 27 n.123 (citing Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 1283 (1975)).

[40] BENNETT & RAAB, *supra* note 5, at xv.

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

and "informational privacy protection" in the United States.[42] These two categories are the closest, if not identical, in their meaning and usage. They are also widely used in the literature on the subject matter.

C. *The Axiological Basis of Normative Regulations: The Euro-Atlantic Community of Values*

My thesis is that the core values that personal data protection regulation seeks to enshrine are very similar, if not identical, in both the United States and in Europe.[43] Personal data (informational privacy) protection is not a goal in itself, but rather, as I set out in the introduction, is of instrumental value, that is, it constitutes one of the cornerstones of a modern democratic society and a significant determinant of individual freedom. Reaching the goal is achieved by ensuring the observance of elementary rules of conduct with regard to personal data processing, which, based on the American literature, I refer to as Fair Information Privacy Practices (FIPPs).[44] I therefore focus on the documents that thus far played an important role in establishing FIPPs, such as the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines), adopted by the OECD in 1980,[45] and the conclusions of the HEW Report of 1973.[46]

1. *OECD Guidelines*

It is a widely held belief that the OECD Guidelines provided a model for modern principles for personal data protection by outlining FIPPs. In spite of

---

[42] I use this term, along with other variations, such as "informational privacy" and "data privacy."

[43] *See, e.g.*, THE SEDONA CONFERENCE, WORKING GRP. SIX, FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY AND E-DISCOVERY app. C (2008), *available at* https://thesedonaconference.org/publication/Framework%20for%20Analysis%20of%20Cross-Border%20Discovery%20Conflicts.

[44] I would like to emphasize two points: (i) the notion of FIPPs/FIPs is not widely used in European literature; (ii) for the purpose of this Article, I will use "data processing" in the European sense, that is "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." EU Data Protection Directive, *supra* note 3, art. 2(b), at 38.

[45] Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)(58)/FINAL (Sept. 23, 1980) [hereinafter *OECD Guidelines*], *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; *see also* PAUL M. SCHWARTZ & DANIEL J. SOLOVE, INFORMATION PRIVACY: STATUTES AND REGULATIONS 2010–2011, at 593 (2010).

[46] HEW REPORT, *supra* note 35, at xix–xxxv.

their non-binding character (they are of indicative value only),[47] the OECD Guidelines have been developed in a creative manner—by being both further clarified/specified and implemented (the most clear expression of which was the adoption, among others, of the Convention No. 108 of the Council of Europe in 1981[48] and the EU Data Protection Directive of 1995), as well as simplified and treated as the foundation of framework regulations.[49] In addition, the global significance of the OECD Guidelines is highlighted by the fact that they were recognized by the United States, which is of particular importance from the point of view of striving for a universal model/framework for regulating personal data protection.

The OECD Guidelines emphasize the need to reconcile the protection of privacy and individual freedom with the free flow of information.[50] They also contain the definition of transborder flows of personal data,[51] setting out detailed instructions on ensuring the free flow of personal data among countries that accepted the Guidelines or adopted them, as well as indications on the scope of reasonable restrictions to free flow of data.[52]

The OECD Guidelines are based on several basic principles (FIPPs):

> Collection Limitation Principle . . . There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> Data Quality Principle . . . Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> Purpose Specification Principle . . . The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

---

[47] JANUSZ BARTA ET AL., OCHRONA DANYCH OSOBOWYCH. KOMENTARZ [PERSONAL DATA PROTECTION: A COMMENTARY] 102 (2007) (translation provided by author); MARIUSZ POLOK, BEZPIECZEŃSTWO DANYCH OSOBOWYCH [PERSONAL DATA SECURITY] 30 (2008) (translation provided by author).

[48] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108.

[49] *See* ASIA-PAC. ECON. COOP., APEC PRIVACY FRAMEWORK 4 (2004), *available at* http://inicio.ifai.org.mx/DocumentosdeInteres/APECPrivacyFramework(Oct-2004).pdf; Graham Greenleaf, *The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?*, 10 PRIVACY L. & BUS. INT'L REP., Jan.–Feb. 2003, at 1.

[50] *See generally OECD Guidelines*, *supra* note 45.

[51] *See id.* ¶ 1; Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217 (2013).

[52] *See OECD Guidelines*, *supra* note 45, ¶¶ 15–18. For more on the subject, please refer to Bygrave, *supra* note 12, at 26–29; Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897 (2013).

> Use Limitation Principle . . . Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
> a) with the consent of the data subject; or
> b) by the authority of law.
>
> Security Safeguards Principle . . . Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> Openness Principle . . . There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> Individual Participation Principle . . . Individuals should have the right:
> a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
> b) to have communicated to them, data relating to them
> i. within a reasonable time;
> ii. at a charge, if any, that is not excessive;
> iii. in a reasonable manner; and
> iv. in a form that is readily intelligible to them;
> c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
> d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> Accountability Principle . . . A data controller should be accountable for complying with measures which give effect to the principles stated above.[53]

I consider that the above rules should be supplemented by the requirement of establishing an independent body dedicated to personal data protection. I should emphasize, however, that such requirement is one of the options prescribed by the OECD Guidelines in order to enforce adherence to FIPPs in practice. The Guidelines suggest "establish[ing] legal, administrative or other procedures *or institutions* for the protection of privacy and individual liberties in respect of personal data."[54] Consequently, pursuant to the EU Data Protection Directive, while implementing it into their respective legal systems, legislators in EU member states established independent personal data protection bodies. For instance, in Poland, the Inspector General for Personal Data Protection (GIODO), with supervisory and investigative powers, is elected by the Polish Parliament for a four-year term.[55]

---

[53] *OECD Guidelines*, *supra* note 45, at Part 2, ¶¶ 7–14, *quoted in* Fred H. Cate, *Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341, 346–47 (Jane K. Winn ed., 2006).

[54] *OECD Guidelines*, *supra* note 45, Part 4, ¶ 19 (emphasis added).

[55] *Poland Data Protection Authority*, CEECPRIVACY.ORG, http://www.ceecprivacy.org/main.php?s=2&k=poland (last visited Sept. 7, 2013).

2. *HEW Report*

The evaluation of the OECD Guidelines would be incomplete if the role of the HEW Report,[56] particularly with reference to FIPPs set out in it, were omitted. I dedicate special attention to the said Report, particularly because its role in the ongoing debate is, in my opinion, underestimated. The influence of the HEW Report is important on several levels and is connected with the timing of the report, the beginning of the 1970s.[57] Although, just as the OECD Guidelines, the HEW Report is a non-binding document, it had a profound impact on the way of thinking about personal data protection, not only in the United States (particularly with reference to the Privacy Act of 1974),[58] but also on the global scale. In my opinion, the HEW Report is an element of the intellectual basis for the OECD Guidelines and reveals a potential framework for legal regulations that is acceptable in the United States. The set of FIPPs presented in the HEW Report encompasses the following principles[59]:

"There must be no personal data record-keeping systems whose very existence is secret."[60] This principle emphasizes the importance of public and individual awareness of the existence of data administrators, as well as data sets maintained by them and data processing systems.

"There must be a way for an individual to find out what information about him is in a record and how it is used."[61] This principle is identified with the requirement to provide information about individuals that the data concerns, a proper notice about data processing and the manner in which they are processed.[62] Analogously to the first principle, it highlights the need to provide reliable information to the individual concerned. In addition, this principle imposes the need to ensure procedural measures to comply with the principle.

"There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent."[63] This principle is also referred to as the "principle of finality" and is connected with the "right of choice."

---

[56] HEW REPORT, *supra* note 35.

[57] The HEW Report was published only three years after the adoption of the first personal data protection act in the world in the German State of Hessen in 1970. *See* Hessisches Datenschutzgesetz [Hessian Data Protection Act], promulgated Oct. 12, 1970, HESSISCHES GESETZ- UND VERORDNUNGSBLATT [HESS GVBL.] at 625 (Hessen) (Ger.). In 1973 Sweden also adopted its personal data protection act. DATALAG [DATA STORAGE] (Svensk författningssamling [SFS] 1973:289) (Swed.).

[58] *See* James B. Rule, *Introduction*, *in* GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION, *supra* note 12, at 4–6.

[59] Cate, *supra* note 53, at 343–44.

[60] HEW REPORT, *supra* note 35, at xx.

[61] *Id.*

[62] *See* Ray Everett-Church, *Privacy Law and the Internet*, *in* GLOBAL PERSPECTIVES IN INFORMATION SECURITY: LEGAL, SOCIAL, AND INTERNATIONAL ISSUES 411–12 (Hossein Bidgoli ed., 2009).

[63] HEW REPORT, *supra* note 35, at xx.

"There must be a way for an individual to correct or amend a record of identifiable information about him"[64] (from which, the "right of access" arises).

"Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data"[65] (connected with broadly defined accountability). In addition, such organizations are required not only to apply measures to ensure security of the data, but also to prevent misuse and inappropriate processing of the data ("reasonable precautions to prevent misuse of the data"[66]). I would therefore be tempted to put forth a thesis that this particular FIPP requires personal data processing entities to act in accordance with fair information practice.

The authors of the HEW Report considered recommending both the establishment of an ombudsman office for personal data protection, as well as a separate federal agency dedicated to data protection; in the end, however, they abandoned this idea altogether. Nevertheless, the interpretation of Section 5 of the FTC Act from the 1990s has consequently resulted in the Federal Trade Commission adopting a *de facto* role of a personal data protection body.[67] I must point out, however, serious legal limitations to the FTC mandate, which allows the agency to act on informational privacy protection breaches only in the case of violations to fair competition.[68] In spite of this, however, I would like to point out the significant systemic measure that brought the American federal model closer to the European one in the systemic and functional aspects.

3. *Comparison of FIPPs Outlined in the HEW Report and in the OECD Guidelines*

A comparison of the FIPPs outlined in the OECD Guidelines and in the HEW Report is, in my opinion, justified, given that it concerns fundamental documents that reveal the system of values protected by ultimate regulation. Table 1 highlights many similarities between the two documents:

---

[64] *Id.*

[65] *Id.* at xxi.

[66] *Id.* at 41.

[67] *See generally* Letter from Marc Rotenberg, Dir., Elec. Privacy Info. Ctr. [EPIC], to Christine Varney, Comm'r, Fed. Trade Comm'n (Dec. 14, 1995), *available at* http://epic.org/privacy/internet/ftc/ftc_letter.html; Memorandum from Paul M. Schwartz & Daniel Solove on The FTC's Role in Privacy Protection: Implications for Food & Beverage Marketing to NPLAN Mktg. to Children Learning Cmty. (June 29, 2009), *available at* http://changelabsolutions.org/sites/default/files/documents/FTC_and_privacy.pdf.

[68] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS ix, 73 (2012).

Table 1: *Comparison of HEW Report and OECD Guidelines*

FIPPs Outlined in the HEW Report	*Corresponding FIPPs Set out in the OECD Guidelines*[69]
a.) "Principle of finality" connected with b.) the principle of "right of choice"	a.) Collection Limitation Principle, b.) Purpose Specification Principle, and c.) Use Limitation Principle
Reliability of the data	Data Quality Principle
a.) Principle stipulating the use of reasonable precautions to prevent misuse of the data, connected with b.) the requirement to implement data safety measures and c.) accountability of the entity processing the data	Security Safeguards Principle
a.) Principle stipulating that there must be no personal-data record-keeping systems whose very existence is secret; b.) principle that there must be a way for an individual to find out what information about him/her is in a record and how it is used; c.) there must be a way for an individual to correct or amend a record of identifiable information about him/her (which entails the "right of access"); and d.) the above-mentioned "right of choice" principle	a.) Openness Principle and b.) Individual Participation Principle
Broadly defined principle of accountability (connected with the above-mentioned principle of the use of reasonable precautions to prevent misuse of the data)	Accountability Principle

Table 1 should also, in my opinion, be supplemented with the requirement of establishing a personal data protection office/agency, as is already the case in EU member states (for example, Inspector General for Personal Data Protection in Poland) and, to some extent, in the United States.[70]

The comparison of the principles contained in the two documents—the HEW Report and the OECD Guidelines—allows us to draw the following conclusions. First of all, there is no full agreement on the scope of principles and their systematics. Second of all, there are no evident contradictions among FIPPs from both groups. Third, each general principle can be identified in both documents. Fourth, given that the OECD Guidelines constitute an axiological source for the EU Data Protection Directive, while at the same time, they derive from the HEW Report, one cannot put forth a thesis that the FIPPs adopted by

[69] I use the term "corresponding," given that the FIPPs are not identical, but rather similar or related, taking into consideration their aims.

[70] See my comments on the role of the FTC, *supra* Part II.C.2.

the European Union stand in absolute contradiction to the American legal system and culture. It is quite the opposite, as evidenced by the chronology of the documents and the FIPPs principles contained therein.

Although the immediate goal of FIPPs is ensuring adequate protection for personal data processed in accordance with norms implementing FIPPs to a given legal system, their intermediate and ultimate goal is protection of fundamental values in a democratic society. The similarity of the FIPPs contained in the HEW Report and the OECD Guidelines is proof that both cultures—European and American—consider similar principles as a guarantee for these values.

By fundamental democratic values I refer to individual freedom, including freedom from unlawful or unreasonable government interference in people's lives,[71] freedom from interference of any other third parties,[72] freedom of expression,[73] as well as the broadly defined principles of individual autonomy and freedom, including the freedom of information.[74] It is therefore paramount to guarantee an individual the right to personality, the right to decide about his/her life (decisional autonomy),[75] the right to self-reflection, self-fulfillment, self-determination, self-evaluation, individuality and self-development,[76] and to ensure an individual the full right to the "shaping of personality and decision-

---

[71] *See, e.g.*, Konstytucja Rzeczypospolitej Polskiej [Constitution], Dz.U. 1997. Nr 78, poz. 483 (as amended), Art. 41, Rozdział II (Pol.), *translated at The Constitution of the Republic of Poland*, SEJM.GOV, http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm (last visited Sept. 3, 2013); U.S. CONST. amend. IV.

[72] *See, e.g.*, Konstytucja Rzeczypospolitej Polskiej, Dz.U. 1997. Nr 78, poz. 483 (as amended), Art. 47, Rozdział II (Pol.); *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 195, 205 (1890) (discussing American legislation and legal doctrine constructed on the basis of the "right to be left alone").

[73] *See, e.g.*, Konstytucja Rzeczypospolitej Polskiej, Dz.U. 1997. Nr 78, poz. 483 (as amended), Art. 54 Rozdział II (Pol.); U.S. CONST. amend. I.

[74] *See generally* WESTIN, *supra* note 41, at 24–26; Andrzej Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)* [*The Conception of the Right to Intimacy and Privacy of Life (Constructive Issues)*], 20 STUDIA CYWILISTYCZNE (1972) (translation provided by author); Irena Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych* [*Constitutional Basis for Personal Data Protection*], *in* OCHRONA DANYCH OSOBOWYCH W POLSCE Z PERSPEKTYWY DZIESIĘCIOLECIA [PERSONAL DATA PROTECTION IN POLAND FROM THE PERSPECTIVE OF THE LAST DECADE] (Paweł Fajgielski ed., 2008) (quoting Wyrok [judgment] TK [Polish Constitutional Tribunal] z [of] Nov. 12, 2002, SK 40/01 (OTK-A 2002, Nr 6, poz. 81)) (translation provided by author); Warren & Brandeis, *supra* note 72.

[75] Safjan, *supra* note 32, at 233.

[76] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906, 1911 (2013); *see also* LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 133–35 (2002); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data than "Privacy,"* ATLANTIC (Jan. 17, 2013, 12:55 PM), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/; Jathan Sadowski, *Why Does Privacy Matter? One Scholar's Answer*, ATLANTIC (Feb. 26, 2013, 12:22 PM), http://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/.

making on personal matters"[77] in the psychological, physical, and social dimensions.[78] The ultimate goal is to provide conditions for the development and proper functioning of a civil society.[79]

These principles, widely accepted in democratic societies, complemented with the rule of law and shared by all legalistic cultures, constitute the Euro-Atlantic community of values,[80] expressed, for example, in the Preamble of the North Atlantic Treaty, signed at Washington on April 4, 1949.[81] The Washington Treaty invokes the need to "safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law."[82] Article 2 of the Treaty emphasizes the need to develop peaceful and friendly international relations by strengthening free institutions, particularly by bringing about a better understanding of the principles upon which these institutions are founded.[83] The signatories of the Treaty, including among others, the United States and Poland, focus rightly on the proper understanding of the functioning of institutions of their partners, pointing out that common aims of countries with different histories, traditions, cultures (including legal), and social structures can be achieved only in such manner.[84] As Polish author Irena Lipowicz points out, the aforementioned invocation contained in the Preamble of the Washington Treaty refers not only to the freedom of a community (nations, societies), but also to individual freedom; it also assumes and emphasizes the existence of a "deposit of common values."[85] A similar stance is presented by the representatives of American authorities that, while looking for convergence, conclude that unchanged, fundamental values around which a transatlantic discussion evolves, are shared by all participants in the Euro-Atlantic debate, and that the common areas in the field of personal data protection and privacy are greater than the

---

[77] Lesław Kański, *Prawo do prywatności, nienaruszalności mieszkania i tajemnicy korespondencji* [*The Right to Privacy, Inviolability of Home and Secrecy of Correspondence*], *in* PRAWA CZŁOWIEKA: MODEL PRAWNY 317, 322 (Roman Wieruszewski ed., 1991) (translation provided by author).

[78] Andrzej Kopff, *Ochrona życia prywatnego w świetle doktryny i orzecznictwa* [*Protection of Private Life in View of Doctrine and Judicature*], 100 ZESZYTY NAUKOWE UNIWERSYTETU JAGIELLOŃSKIEGO PRACE PRAWNICZE 37 (1982) (translation provided by author).

[79] For similar views see Aditi Bagchi, *Deliberative Autonomy and Legitimate State Purpose Under the First Amendment*, 68 ALB. L. REV. 815, 815 (2005); James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 30–56 (1995).

[80] *See* Irena Lipowicz, *NATO a wartości* [*NATO and Values*], *in* SUWERENNOŚĆ I INTEGRACJA EUROPEJSKA, MATERIAŁY POKONFERENCYJNE [SOVEREIGNTY AND EUROPEAN INTEGRATION, POST-CONFERENCE PUBLICATION] (Władysław Czapliński et al. eds., 1999) (translation provided by author).

[81] North Atlantic Treaty pmbl., Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[82] *Id.*

[83] *Id.* art. 2.

[84] *Id.*

[85] Lipowicz, *supra* note 80.

underlying differences.[86] I will examine these differences in the section that follows.

D. *Systemic Differences*

In this section I will focus on the fundamental differences between the European (including Polish) and the American personal data and informational privacy protection systems. Basic characteristics of the European system can be summarized in several points. In the part that follows, I will present a model approach, in order to subsequently evaluate the practical use and directions in which these models evolve. At the same time, I would like to make clear that I focus on statutory law sources, without delving into the analysis of case law which is the basis of the common law system.

I would like to signal, however, that when evaluating the adequacy of non-European legal systems with regard to personal data protection, vis-à-vis European regulations, one should take into account the overall picture, including a non-European judicature. In my opinion, this aspect is often overlooked, given that traditionally only statutory regulations are analyzed, in spite of the importance of legal decisions in the common law. At the same time, I am only referring here to general regulations on the protection of individuals with regard to the processing of personal data and on the free movement of such data, without taking into consideration specific regulations on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection, or prosecution of criminal offences and terrorism.

1. *Statutory Law Sources in the Area of Personal Data Protection and Informational Privacy: A Model Approach*

The European system of personal data protection adopts the principle of compiling all norms regulating the entire area of data protection in one legal act functioning as a sort of "constitution" for the entire field (both in public and private sectors), with its normative basis in the highest legal acts. It is often referred to as an omnibus regulation, covering both public and private sector entities. At the European Union level, the regulation that is the basis for the personal data protection system is the EU Personal Data Protection Directive

---

[86] Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Speech at the EU Conference on Privacy and Protection of Personal Data (Mar. 19, 2012); David Vladeck, Dir., Fed. Trade Comm'n, Bureau of Consumer Prot., Participant at the EU Conference on Privacy and Protection of Personal Data (Mar. 19, 2012); Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., Fed. Trade Comm'n, Participant at the EU Conference on Privacy and Protection of Personal Data (Mar. 19, 2012); Rep. Ed Markey (D-MA), Co-Chair of Cong. Privacy Caucus, Keynote Speech at the EU Conference on Privacy and Protection of Personal Data (Mar. 19, 2012). These presentations are available at http://scic.ec.europa.eu/streaming/indexh264.php?es=2&sessionno=0cdf61037d7053ca59347ab230818335.

95/46 (with its primary sources in the Treaty on European Union, the Treaty on the Functioning of the European Union, and the Charter of Fundamental Rights of the European Union).[87] In Poland, such regulation is the Personal Data Protection Act of 1997,[88] implementing the norms of the Directive 95/46, with its national basis in Article 51 of the Constitution of the Republic of Poland.[89] The adoption of a relatively homogenous (omnibus) regulation, with a consistent (which does not imply flawless) structure, is meant to facilitate applying these norms in practice. This does not mean, however, that a particular legal act does not stipulate different, usually enhanced, personal data protection in specific areas.[90]

The American system is characterized by regulatory fragmentation ("patchwork," "kaleidoscopic," and "mosaic approach"), mainly because there is no single fundamental legal act regulating the entire area of informational privacy in a complex and framework manner. The exception to this rule is the Privacy Act of 1974, which remains the fundamental legal act in the area of privacy and personal data protection on the federal level, albeit limited in scope to a certain area of the public sector; hence it is without a fully universal character.[91]

---

[87] Charter of Fundamental Rights of the European Union, Dec. 7, 2000, 2012 O.J. (C 326) 391; Treaty on European Union, Feb. 7, 1992, 2012 O.J. (C 326) 13; Treaty on the Functioning of the European Union, Mar. 25, 1957, 2012 O.J. (C 326) 47; Irena Lipowicz, *Polska administracja publiczna w świetle standardów europejskich* [*Polish Public Administration in View of European Standards*], *in* PRAWO ADMINISTRACYJNE [ADMINISTRATIVE LAW] 334, 344–45 (Zygmunt Niewiadomski ed., 2011) (translation provided by author).

[88] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [Polish Data Protection Act of 1997] (1997 r. Dz.U. Nr 133, poz. 883 as amended).

[89] Konstytucja Rzeczypospolitej Polskiej [Constitution] Dz.U. 1997 Nr 78, poz. 483 (as amended), Art. 41 (Pol.), *translated at The Constitution of the Republic of Poland*, SEJM.GOV, http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm (last visited Sept. 3, 2013).

[90] 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 (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37; Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1; *see also* Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny [Polish Civil Code 1964] (1964 r. Dz.U. Nr 16, poz. 93 as amended); Ustawa z dnia 22 maja 2003 r. o działalności ubezpieczeniowej [Polish Insurance Act] (2003 r. Dz.U. Nr 124, poz. 1151 as amended); Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne [Polish Telecommunications Act] (2004 r. Dz.U. Nr 171, poz. 1800 as amended); Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej [Polish Freedom of Information Act] (2001 r. Dz.U. Nr 112, poz. 1198 as amended).

[91] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2012)).

Other federal informational privacy protection acts are sector-specific.[92] Such fragmentation of norms may theoretically result in difficulties in applying them in everyday life.[93]

However, similar shortcomings are also inherent in the European legal system, which I have encountered on numerous occasions in my legal practice. In the section that follows, I will describe regulation methods in Europe (including Poland) and in the United States.

2. *Regulation Methods in the Model Approach*

The European system of personal data protection is based on an administrative method, characterized by the ability of neutralizing any asymmetry among different entities. European literature explains that traditional (civil and criminal law) data protection methods and mechanisms turned out to be ineffective in their preventive function, hence the onus on protecting individuals and their privacy is moving markedly towards institutional, public law measures.[94] In other words, the administrative method is used when there is a need to "level the playing field" and to lend support for formally weaker

---

[92] REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005) (codified as amended at 8 U.S.C. § 1778 (2012)); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified as amended in scattered sections of 15 U.S.C., 20 U.S.C. §§ 9701–9708 (2002)); Children's Online Privacy Protection Act (COPPA) of 1998, Pub. L. No. 105-227, 112 Stat. 2681–2728 (1998) (codified at 15 U.S.C. §§ 6501–6506 (2012)); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 and 42 U.S.C.); Drivers Privacy Protection Act, Pub. L. No. 103-322, 108 Stat. 2102 (1994) (codified as amended at 18 U.S.C. § 2721 (2012)); Video Privacy Protection Act, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 47 U.S.C. § 2710 (2006)); Employee Polygraph Protection Act of 1988, Pub. L. No. 100-347, 102 Stat. 646 (1988) (codified as amended at 29 U.S.C. § 2001 (2006)); Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (1980) (codified as amended at 42 U.S.C. § 2000aa (2006)); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2012)); Fair Credit Reporting Act, ch. 41, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. § 1681 (2012)); Electronic Communications Privacy Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)); Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552 (2012)); Federal Trade Commission Act, ch. 2, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41–58 (2012)); Child Online Protection Act (COPA), 112 Stat. 2681-736, Pub. L. No. 105-277 (1998) (codified as amended at 47 U.S.C. § 231 (2006)), *invalidated by* Ashcroft v. ACLU, 542 U.S. 656, 673 (2004); *see also* Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029, 1035–36 (2013).

[93] For similar views, see PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW xvii (3d ed. 2009); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 208–09 (1992); *see also* Priscilla M. Regan, *The United States*, *in* GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION, *supra* note 12, at 50, 74–76.

[94] Safjan, *supra* note 11, at 5–7.

players in their relations with authorities (vertical relations) or with other formally more powerful entities, such as businesses (horizontal relations). The elimination of imbalance is achieved mainly through the involvement and the exercise of power by the state.[95] Hence there is the presence of independent personal data protection bodies in the European system, with supervisory and ombudsman competencies (including the power to undertake actions to protect individuals' interests). Such bodies may initiate actions *ex officio*, and apply different sanctions. For example, the Polish Inspector General for the Protection of Personal Data, although not vested with powers to impose financial penalties,[96] may, among other powers, prohibit the transfer of personal data from Poland to any third countries (including the United States) or order the deletion of personal data.[97] Such orders can obviously have a serious impact on operations of businesses.

A different regulation method is used and popularized in the United States, particularly in the vertical relations sphere, where the emphasis is on private law mechanisms, including self-regulation and self-certification.[98] In this model, authorities (particularly the judiciary) intervene in cases of a breach of accepted practices only if the proceedings are initiated by an individual. In this model generally there is no special body dedicated exclusively to personal data protection (any specialized agencies act as organizational units of other bodies, such as consumer protection agencies).[99] Such a regulation method stems from the assumption that in a free market economy, private law measures, along with judicial oversight of informational privacy protection, provide adequate personal data protection. Nevertheless, the public law method can be observed in the public sector.[100]

---

[95] *See, e.g.*, ZBIGNIEW LEOŃSKI, MATERIALNE PRAWO ADMINISTRACYJNE [MATERIAL ADMINISTRATIVE LAW] 12 (2000) (translation provided by author); EUGENIUSZ OCHENDOWSKI, PRAWO ADMINISTRACYJNE, CZĘŚĆ OGÓLNA [ADMINISTRATIVE LAW: GENERAL PART] 35–36 (2000) (translation provided by author); HARTMUT MAURER, OGÓLNE PRAWO ADMINISTRACYJNE (ALLGEMEINES VERWALTUNGSRECHT) 40 (2003); PRAWO ADMINISTRACYJNE [ADMINISTRATIVE LAW], *supra* note 87, at 94; Grażyna Szpor, *Publicznoprawna ochrona danych osobowych* [*Personal Data Protection in Public Law*], 12 PRZEGLĄD USTAWODAWSTWA GOSPODARCZEGO 2, 10 (1999) (translation provided by author).

[96] It can, however, refer cases to the public prosecutor's office, as violations of personal data protection are a criminal offense subject to imprisonment of up to three years.

[97] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [Polish Data Protection Act of 1997] (1997 r. Dz.U. Nr 133, poz. 883, Art. 18.1, as amended).

[98] SWIRE & AHMAD, *supra* note 30, at 32–33.

[99] See, e.g., state offices in California, where the Information Security Office is a part of the California Department of Technology, the Office of Privacy Protection is a part of the State and Consumer Services Agency, and the Division of Privacy and Identity Protection is a part of the Federal Trade Commission (FTC). *See generally* Tal Z. Zarsky & Norberto Nuno Gomes de Andrade, *Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum*, 74 OHIO ST. L.J. 1335 (2013).

[100] *See, e.g.*, Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (2012)).

3. *Evaluation of Regulation Methods in the Model Approach*[101]

The method described above as "European" has its advantages. The regulation is matter-of-fact, easy to navigate for individuals, relatively transparent and homogeneous, offering support of specialized administrative bodies dedicated exclusively to personal data protection. It also has its shortcomings, which stem from its inflexibility, which in turn may limit innovations in the economy. As is the case with all regulations in the fast-changing economy, it is likely to result in normative gaps (given ongoing technological developments impossible to foresee at the time a given regulation is adopted), excessive discretionary powers granted to the personal data protection body attempting to fill the said gaps, as well as low tolerance for different legal solutions, considered *a priori* as less effective in protecting personal data (which constitutes an evaluation method for European regulation, rather than an inherent characteristic of such method).[102] Moreover, we can observe a growing trend of juridification of areas which until recently were free from public interference,[103] which is a tendency to regulate each sphere of life by means of administrative regulations.

Among the advantages of the method described as "American" are flexibility, which is conducive to the development of an innovative economy, the ability to adapt to a fast-changing environment (including technological advances),[104] and leaving the power of initiative and freedom to individuals. Among its drawbacks, we should include putting the onus of protecting their rights on individuals, who, in the vast majority, have limited resources (financial, technical, organizational, etc.) in comparison with administrative authorities and business entities. In the U.S. model, there is also a risk of passiveness toward violations of personal data processing rules that may result from subjectively viewed harmlessness of individual informational privacy breaches (individual breaches may seem negligible, but the accumulation thereof, the so-called "aggregation effect,"[105] is not). In addition, sector regulation ("patchwork," "kaleidoscopic," and "mosaic approach") results in

---

[101] For an in-depth analysis of the advantages and disadvantages of the regulation models please see SWIRE & AHMAD, *supra* note 30, at 30–44.

[102] *Id.* at 31.

[103] Szpor, *supra* note 95, at 12.

[104] According to Polish scholar Roman Tokarczyk, common law "knows no normative gaps, given that new cases result in new precedents," while in statutory law some normative gaps are unavoidable. *See* ROMAN TOKARCZYK, WSPÓŁCZESNE KULTURY PRAWNE [CONTEMPORARY LEGAL CULTURES] 143 (2010) (translation provided by author).

[105] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 27 (2011); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 44–47 (2004); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 117–21 (2008); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1184–95 (2002). This phenomenon is well illustrated by the maxim "the whole is greater than the sum of its parts."

difficulties in everyday application of the law,[106] while self-regulation by business entities may lead to personal data protection standards reflecting business needs and interests, which often differ from those of individuals.[107]

4. *Reasons Behind Regulatory Differences*

As shown in my analysis, in spite of important similarities (or in some cases virtual uniformity) of the fundamentals of both systems on the axiological level,[108] there are significant differences on the level of specific regulations, as summarized in the preceding section. As Paul M. Schwartz and Joel R. Reidenberg rightly point out, although from the legal point of view personal data protection in the EU and the United States may be identical in some cases, the manner in which it is ensured is normally quite different.[109]

In the European doctrine, personal data protection stems from the common root of inalienable human rights and fundamental rights. Several authors when referring to these rights within the context of the European regulations associate them with "dignity," "respect," "honor," "inalienable rights," "dignitary interests," "fundamental rights," "basic human rights," and "fundamental human rights."[110] The reference to "dignity" is very significant, in my opinion. To quote Marek Safjan, a distinguished Polish researcher and expert on the subject, and the former President of the Polish Constitutional Tribunal, "dignity is a primary right . . . [and] source of any and every other right."[111] Privacy, including informational privacy and personal data protection, should fall under special protection because of its very nature and connection with the freedom and right to self-determination of an individual.[112] Because of historical, cultural, and sociological factors, discussion on this subject in Europe is taking place on the elementary values layer (such as dignity and freedom). European

---

[106] For similar views, see CAREY, *supra* note 93; Reidenberg, *supra* note 93; *see also* Regan, *supra* note 93.

[107] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 19.

[108] *See supra* Table 1.

[109] SCHWARTZ & REIDENBERG, *supra* note 14, at 24–25, 342, 395–96.

[110] SOLOVE & SCHWARTZ, *supra* note 38, at 15; Cate, *supra* note 12, at 179, 225–26; Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493, 562–63 (2007); Whitman, *supra* note 31, at 1161, 1214; Gabriela Zanfir, *EU and US Data Protection Reforms. A Comparative View*, 7 EUR. INTEGRATION REALITIES & PERSP. 217, 217–19 (2012); Kobrin, *supra* note 12, at 27; Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923 (2013).

[111] Safjan, *supra* note 32, at 227, 237.

[112] Marek Safjan, Prawo do ochrony życia prywatnego [The Right to Protection of Private Life], *in* HELSIŃSKIEJ FUNDACJI PRAW CZŁOWIEKA [HELSINKI COMMITTEE FOR HUMAN RIGHTS], SZKOŁA PRAW CZŁOWIEKA [HUMAN RIGHTS SCHOOL] 211, 212, 214, 222 (1996) (translation provided by author).

sociology also regards the said values as fundamental.[113] "The dignity of human being" is treated as the "essence of human being . . . the cornerstone of the entire constitutional order . . . basic norm (*Grundnorm*), and its source is 'humanness' *per se*."[114]

In the United States, on the other hand, the issue of informational privacy is linked with liberty values, understood not only as "freedom from" (surveillance or interference of third parties), but also "liberty to" (actions, manifestations of ingenuity).[115] The American legal system also recognizes fundamental values and human rights.[116] The most recent American literature in particular recognizes privacy as a social good that contributes to the shaping of a democratic civil society.[117] Nonetheless, the American system tends to take into account purely practical, economic value of personal data, as an intangible, legal value that may be subject to business transactions as an alienable commodity.[118] Such a pragmatic point of view is also illustrated by Jerry L. Mashaw, according to whom "[t]he question is not what rights are natural to persons, but what rights persons must have to maintain a particular liberal and democratic polity."[119]

In my opinion, the source of the said differences is divergent views on the role of an individual and his/her position in society, stemming from distinct historical, social, and cultural experiences, as well as geographic location. This dissimilarity, in my view, clearly affects specific regulations on personal data (informational privacy) protection in Europe and the United States. Public law regulation in Europe is protectionist and paternalistic, providing individuals with care and protection *ex officio*. An individual, from the angle of European experiences and conditions, is regarded as the subject of fundamental human rights—vulnerable victim of potential abuse by the more powerful (including, for example, authorities and/or business entities).

On the other hand, American informational privacy protection regulations are characterized by their pragmatism and a pro-market approach. In the American system, the individual is treated as a conscious participant in legal and economic relations, or in other words, as a consumer. Consumers can seek

---

[113] Zygmunt Bauman, Professor, Postmodernistyczny obraz człowieka w społeczeństwie. Gdzie źródła nadziei na lepszą przyszłość? [A Postmodern Image of a Human Being in Society: Where Can Sources of Hope for a Better Future Be Found?] (presented at Lecture at the IV Kongres Kultury Chrześcijańskiej, Sept. 29, 2012).

[114] Bartosz Wojciechowski, *Prawa człowieka jako element polityki wzajemnego uznania i równości szans* [*Human Rights as a Policy of Mutual Recognition and Equal Opportunity*], *in* KONWERGENCJA CZY DYWERGENCJA KULTUR I SYSTEMÓW PRAWNYCH? 115 (Oktawian Nawrot, Sebastian Sykuna & Jerzy Zajadło eds., 2012) (translation provided by author).

[115] Zanfir, *supra* note 110, at 218.

[116] ANCEL, *supra* note 32, at 104.

[117] Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2180–82 (2003).

[118] CRAIG & LUDLOFF, *supra* note 9, at 30, 50, 78–79; Kobrin, *supra* note 12, at 8, 23.

[119] JERRY L. MASHAW, DUE PROCESS IN THE ADMINISTRATIVE STATE 169 (1985), *quoted in* SCHWARTZ & REIDENBERG, *supra* note 14, at 65.

their rights through the judicial system using legal instruments provided by the state. This view of individuals and their position in the legal system is the function and consequence of the basic principles on which the United States was founded and developed.

a. *Privacy Paradox No. 1*

The above observations illustrate one of the privacy paradoxes, that is the conclusion that, in spite of common axiological foundations and, in principle, identical value systems, the normative solutions aimed at protecting such values applied in different countries may be quite different.

The reasons behind these differences may stream from well-established factors outside the legal system, such as historical, social, cultural, geographic, or linguistic. Such factors and conditions result in different placement of emphasis and priorities that subsequently are implemented by legislators in order to protect fundamental, Western civilization values.

b. *Privacy Paradox No. 2*

The characteristics of the European and American personal data protection systems presented above apply to traditional models, which in practice lose their purity and absorb each other's features. For example, personal data protection regulation in Europe loses its homogeneous character, and the area becomes increasingly regulated by detailed regulations/legal acts (applying to a specific sector). Thus the simplicity of the regulation is being lost, prompting erosion of the system in this area. As noted by Irena Lipowicz, we are currently witnessing the process of marginalization of the Act on Personal Data Protection in Poland, which is no longer a bind holding the entire regulation as one logical and coherent entity.[120] We are therefore witnessing a fragmentation and dispersal of regulation, which is characteristic of the American system. Another trend that can be observed in Europe is the permeation of civil law instruments into the traditional public law regulation. What I refer to are, for example, co-regulative measures, such as the agreements between the Polish Inspector General for the Protection of Personal Data and the Polish Association of Direct Marketing (2008) or the Polish Automotive Industry Association (2012), which outline the code of good business practices on personal data protection in their respective sectors.[121] Similar civil law measures are applied

---

[120] Irena Lipowicz, *Nowe wyzwania w zakresie ochrony danych osobowych* [*Personal Data Protection: New Challenges*], *in* INTERNET. OCHRONA WOLNOŚCI, WŁASNOŚCI I BEZPIECZEŃSTWA 3, 14 (Grażyna Szpor ed., 2011) (translation provided by author); *see also* Wojciechowski, *supra* note 114, at 122–23.

[121] GENERALNYM INSPEKTOREM OCHRONY DANYCH OSOBOWYCH, POROZUMIENIE POMIĘDZY GENERALNYM INSPEKTOREM OCHRONY DANYCH OSOBOWYCH A PREZESEM POLSKIEGO ZWIĄZKU PRZEMYSŁU MOTORYZACYJNEGO [AGREEMENT BETWEEN THE POLISH INSPECTOR GENERAL FOR THE PROTECTION OF PERSONAL DATA AND THE AUTOMOTIVE

on the EU level—for example, the model Standard Contractual Clauses or Binding Corporate Rules,[122] which provide for varying levels of involvement of administrative bodies, are based on contractual schemes. Until quite recently, solutions of such type were non-existent in the traditional, public model of social regulations.

The American system is also undergoing noticeable changes, the most important of which is the increased activity of the Federal Trade Commission in the area of personal data protection. The FTC has demonstrated an inclination to initiate proceedings *ex officio*, anticipating individual actions, which brings the American model closer to the European one, increasing the degree of protectionism.[123]

The above observations lead me to another privacy paradox, which is the conviction among the participants in the transatlantic debate of the superiority of their respective systemic solutions. In reality, however, these solutions are gradually evolving and the instruments of both legal cultures start to blend with each other. Such process, although slow and long-lasting, is a manifestation of the strength and "healthiness" of both legal systems, and constitutes a legislative response to new challenges, particularly social phenomena arising from the development of new technologies used for collecting and processing personal data.[124]

INDUSTRY ASSOCIATION] (Nov. 16, 2012), *available at* www.giodo.gov.pl/plik/id_p/3068/j/pl/ (translation provided by author).

[122] Standard Contractual Clauses and Binding Corporate Rules are EU measures designated to allow transfer of personal data from the territory of the EU to other countries, such as the United States. For more information on the subject, please see SWIRE & AHMAD, *supra* note 30, at 36–37.

[123] I refer, in particular, to FTC proceedings against Google, Inc. and Facebook, Inc., which may be considered as actions on behalf of all consumers in the world. For more information on this subject, please see Lesley Fair, *Milking Cookies: The FTC's $22.5 Million Settlement with Google*, BUREAU CONSUMER PROTECTION BUS. CENTER BLOG (Aug. 9, 2012, 11:02 AM), http://business.ftc.gov/blog/2012/08/milking-cookies-ftcs-225-million-settlement-google; *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees To Implement Comprehensive Privacy Program To Protect Consumer Data*, FED. TRADE COMMISSION (Mar. 30, 2011), http://www.ftc.gov/opa/2011/03/google.shtm; *FTC Approves Final Settlement with Facebook: Facebook Must Obtain Consumers' Consent Before Sharing Their Information Beyond Established Privacy Settings*, FED. TRADE COMMISSION (Aug. 10, 2012), http://ftc.gov/opa/2012/08/facebook.shtm.

[124] I refer to the already mentioned phenomena, such as Big Data and Open Data. *See e.g.*, Case C-138/11, Compass-Datenbank GmbH v. Republik Österreich, 2011 EUR-Lex CELEX LEXIS 0138 (July 12, 2012), *available at* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=req&docid=124999&occ=first&dir=&cid=6123250; CRAIG & LUDLOFF, *supra* note 9, at 4; MAYER-SCHÖNBERGER & CUKIER, *supra* note 9, at 2, 116; Kuner et al., *supra* note 9, at 47–48; Marcinkowski & Kuca, *supra* note 9.

III. IN SEARCH OF CONVERGENCE: A GLOBAL VISION OF PERSONAL DATA PROTECTION

Given its importance in today's world, the controversial field of personal data protection and transborder data transfers not only deserves attention, but also requires transcontinental solutions.

For the last few decades, both Europe and North America have been developing complex and diverging systems aimed at protecting the same fundamental values. The overall regulations (*acquis*) and experience will not allow any revolutionary changes to take place (such as the United States adopting the EU Personal Data Protection Directive or the European Union giving up institutional measures of the Directive 95/46 for the sake of self-regulation). The political debate that is currently taking place suggests that negotiations have arrived at the "point of no return" and the representatives of both sides treat the negotiations as a matter of *de facto* non-negotiable principles, as they consider them. Theoretically, interesting and particularly innovative proposals, such as setting up a "National Information Market"[125] or introducing a system of licenses that authorize administrating computer systems,[126] have a slim chance of materializing.[127]

I am, therefore, inclined to propose developing solutions streaming from the European and American laws and experiences. The starting point, in my view, should be the realization of divergence of the current, respective personal data protection systems and the emphasis on common values. Such understanding would provide a stepping stone for a Euro-Atlantic personal data (informational privacy) protection system, adopting a co-regulative method.

I assume that co-regulation stipulates a broad use of civil law mechanisms and measures, along with public law mechanisms and solutions. Therefore, codes of good practices drawn up by business circles (civil law element) should fall under the supervision (at the project and implementation stage) of data protection authorities or special agencies within the existing administrative bodies providing public supervision and enforcement, also initiated *ex officio*. It is also necessary to ensure effective international cooperation of the said bodies,[128] at least within an informal trans-governmental administrative network,[129] ensuring the right for consumers to seek individual redress abroad.

---

[125] Kenneth C. Laudon, *Markets and Privacy*, 39 COMM. ACM 92, 99–103 (1996).

[126] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 242–45 (1971).

[127] For a similar view, see Christopher Kuner, *An International Legal Framework for Data Protection: Issues and Prospects*, 25 COMPUTER L. & SECURITY REV. 307, 315 (2009).

[128] For more on this subject, see SWIRE & LITAN, *supra* note 7, at 156–58.

[129] SWIRE & AHMAD, *supra* note 30, at 61; Christopher Kuner, *Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future* 7–8 (Tilburg Inst. for Law, Tech. & Soc'y, Working Paper No. 016, 2010). It should be noted that in the past, data protection bodies from the EU initiated proceedings in the United States—for example, the German Federal Data Protection Commission carried out such proceedings, with the consent of the company, at Citibank's headquarters. For more

In the case of unavailability of civil law measures (such as codes of good practices), international FIPPs principles would apply, established on the basis of analytical comparisons, such as the one presented in Table 1, ensuring public supervision and public enforcement.

It would also be appropriate to supplement the proposed model with the principle of accountability and responsibility for data exporters. Such exporters would be accountable for data processing by the importer abroad, including possibly further processing in a way incompatible with initial purposes and onward transfers.[130] Additional features, such as Privacy by Default and Privacy by Design, should be provided by technological measures.[131] I believe that in this way we could achieve the interoperability of diverging systems.

I do not claim that the proposed solution would satisfy all needs. In my opinion, however, it may be a starting point for reaching a solution that is acceptable for all participants in the debate (an "imperfect agreement"), offering a way out from a negotiating impasse.

If no constructive solution or concept of how to face Privacy Paradoxes is offered, we will either face a standstill in the Euro-Atlantic economic, scientific, and cultural relations (which I doubt),[132] or our personal data protection will only be superficial and illusory. In either of these cases, the fundamental Euro-Atlantic values would come under a serious threat.

---

information, please see Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, 18 INT'L J.L. & INFO. TECH. 227, 232–34 (2010).

[130] *See* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 173–74 (2013); Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, *in* REINVENTING DATA PROTECTION? 263, 269–72 (Serge Gutwirth et al. eds., 2009); Christopher Kuner, Global Data Transfers on the Internet: Lessons from the Ancient World 5 (Aug. 4, 2009) (unpublished working paper), *available at* http://ssrn.com/abstract=1445458.

[131] *See* WOJCIECH WIEWIÓROWSKI, GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH, NOWE EUROPEJSKIE REGULACJE W ZAKRESIE PRYWATNOŚCI W FAZIE PROJEKTOWANIA I PRYWATNOŚCI W DOMYŚLNYCH USTAWIENIACH [NEW EUROPEAN REGULATIONS ON PRIVACY BY DESIGN AND PRIVACY BY DEFAULT SETTINGS] (Mar. 7, 2012), *available at* http://www.giodo.gov.pl/plik/id_p/2646/j/pl/ (translation provided by author).

[132] Particularly taking into account the proposed EU–U.S. Transatlantic Trade and Investment Partnership. *See* European Comm'n, *United States*, COUNTRIES & REGIONS, http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/ (last updated June 18, 2013).