DOES UKRAINE NEED A COMPREHENSIVE STATUTE TO "CONTROL" PRIVATE DATA CONTROLLERS?

OLENA DMYTRENKO*
CARA D. CUTLER**

ABSTRACT

This Article considers whether a European Union model of data protection, predominately in the form of a comprehensive statute, or a U.S. model of data protection, favoring industry self-regulation enhanced by sectoral legislation, would be best for Ukraine. This Article argues that a comprehensive statute may fit more easily into Ukraine's civil law culture and may prove to be a requirement necessary for the country to obtain its goal of accession to the European Union. However, until Ukraine builds a strong democratic legacy, a rapid transplant of the European Union-style comprehensive statute may be detrimental to nurturing nascent private businesses and independent media. The Article argues that Ukraine's short-term success demands adoption of a self-regulatory model akin to that of the United States for the time being. At the same time, slow steps should be taken to begin assessing whether or not implementation of a comprehensive statute in the future will suit Ukraine's long-term needs.

I. INTRODUCTION

Western civilization altered social interactions in the twentieth century simultaneously in two opposing directions. On the one hand, humankind developed sophisticated technology for collecting, compiling, analyzing, and sharing information about people. On the other hand, people increasingly grew to respect human individuality and independent mental

* Junior Attorney at the Kyiv, Ukraine office of Baker & McKenzie. LL.M. (2004), *with honors*, University of Washington School of Law; Master of Laws (2001), *highest honors,* Shevchenko National University, Kyiv, Ukraine.

** Member of the New York Bar. LL.M. (2005), University of Washington School of Law; J.D. (2004), *cum laude*, University of Connecticut School of Law; B.A. (2001), *cum laude*, Connecticut College.

experimentation, which inevitably led to shared acknowledgement of a right to be left alone.

Technological advances triggered public concern about individual privacy and demanded that legal systems respond by creating means to protect personal data, information related to identified or identifiable individuals.[1] Not only national legal systems, but also the global international community, reacted to the new challenge by adopting relevant legal instruments. The 1948 United Nations Universal Declaration of Human Rights[2] and the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) recognized privacy as a fundamental human right.[3] In the 1960s, the right to privacy began to be given explicit protection in the United States, through the Supreme Court's decisions in *Mapp v. Ohio*[4] and *Griswold v. Connecticut*.[5] In 1980, the Organization for Economic Cooperation and Development (OECD), with the world's thirty largest economies signing on as members, adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[6] The *Guidelines'* objective is to reconcile the fundamental but competing values such as privacy and the free flow of information.[7] The following year, the Council of Europe followed suit by enacting the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[8]

While the twentieth century brought the recognition of a fundamental right to privacy to both the United States and the European Union, the two developed distinct approaches to protecting this right. To prevent these differences from impeding the transatlantic information flow, the two

---

1. *See, e.g.*, Organization for Economic Cooperation and Development [OECD], *Recommendation Concerning And Guidelines Governing The Protection of Privacy And Transborder Flows of Personal Data*, O.E.C.D. Doc. C(80)58(Final) (Oct. 1, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 5, 2006) [hereinafter OECD Guidelines].

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

3. Eur. Consult. Ass. [ECHR], *Convention for the Protection of Human Rights and Fundamental Freedoms*, GETS No. 005, art. 8 (Nov. 4, 1950), *available at* http://conventions.coe.int/Treaty/er/Treaties/Html/005.htm (last visited Jan. 5, 2006).

4. 367 U.S. 643, 656 (1961) (stating that the Fourth Amendment creates "right to privacy, no less important than any other right carefully and particularly reserved to the people").

5. 381 U.S. 479, 484 (1965) (finding that the First, Third, Fourth, Fifth, and Ninth Amendments each provide certain rights or guarantees and that these "various guarantees create zones of privacy").

6. OECD Guidelines, *supra* note 1.

7. *Id.* pmbl.

8. Eur. Consult. Ass., *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Doc. No. 108 (Jan. 28, 1981), *available at* http://convention.coe.nt/Treaty/er/Treaties/Html/108.htm (last visited Jan. 23, 2006) [hereinafter COE Convention].

sides began to engage in a safe harbor arrangement. A safe harbor arrangement was necessary for both the United States and the EU because "the United States and the European Union share the goal of enhancing privacy protection for their citizens, [but] the United States takes a different approach to privacy from that taken by the European Union."[9] The U.S. approach to protection of privacy relies on the philosophy that regulation of private data controllers is based on protecting personal information as a valuable asset and, by default, relies on market self-regulation.[10] By contrast, the EU treats data protection as a fundamental, universal human right and advocates an "omnibus"[11] proactive statute for regulating private controllers.

Ukraine was essentially immune from the data protection issues facing the EU and the United States until its independence in 1991. Faced with independence, Ukraine abandoned the coziness of the Iron Curtain in exchange for freedom. However, its legal system was caught naked and unprepared. The country proclaimed a policy of furthering a western-style democracy, with a western-style legal system[12] for integration into the world economy.[13]

The free market economy, liberalized information flows, computer technology, and human rights protection rushed rapidly and forcefully into Ukraine. Along with these changes, as in the EU and the United States, Ukraine was faced with the task of determining how its legal system should protect personal data from misuse by private controllers. The choice arises between providing centralized involvement of the

---

9. U.S. DEP'T OF COMMERCE, SAFE HARBOR PRINCIPLES (July 21, 2000), *available at* http://www.export.gov/safeharbor/SHPRINCIPLEFINAL.htm.

10. James P. Nefh, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 2 (2005). Nefh states:

> By doing little to regulate information privacy outside government agencies, Congress defaulted to a voluntary, market-oriented model that relied on individual self-policing as the dominant means of information control, supplemented in later years by state laws and federal sector-specific legislation. Proposals for a federal "privacy board" that would oversee a national policy, for example, were rejected . . . . To this day, information privacy in the United States relies heavily on individuals guarding the integrity of their data records and protecting personal information from unintended use.

Id. (internal citations omitted).

11. DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 687 (Aspen Publishers 2003).

12. Anna M. Kuzmik, *Rule of Law and Legal Reform in Ukraine*, 34 HARV. INT'L L.J. 611, 611 (1993) ("[O]ne of the central themes of reform has been the transition from a socialist legal regime, to a regime based on the western concept of 'rule of law.'").

13. KONSTITUTSIJA UKRAJINY [Ukr. Constitution]. *See* Official English Translation of the Constitution of Ukraine, *available at* http://www.rada.kiev.ua/const (last visited Jan. 5, 2006) [hereinafter UKR. CONST.].

government through a comprehensive data-protection statute, as the EU does, and leaving the matter largely to self-regulation between private parties, as in the United States.

Currently, Ukraine is at a fork in the decision-making road. This Article explores the issue, suggests a suitable short term solution for Ukraine, and stresses the importance of avoiding premature implementation of a data-protection statute. Why is the question of a comprehensive statute on protecting data from private controllers so critical for Ukraine today? This question is resolved differently in two contrasting legal orders: the statutory order of the EU and the self-regulatory order of the United States. Each has strengths and weaknesses, and this paper discusses which approach is more appropriate for Ukraine.

II. DATA PROTECTION IN UKRAINE

A. Ukraine Within the Soviet Union

When Ukraine was part of the Soviet Union, the question of controlling private data protection was not one for a legal system at all. The country was engaged in building communism, and, as part of this process, it possessed the long-term goal of abandoning law altogether.[14] Communist ideology deems law a tool necessary only in antagonistic, imperfect societies.[15] However, during its transition to true communism, while Soviet society was still somewhat imperfect, use of law was felt to be acceptable for the short term.

It would be unfair to say that law offered no protection to personal data. The USSR Constitution established that "[t]he privacy of citizens, and of their correspondence, telephone conversations and telegraphic communications is protected by law."[16] However, this was not a constitutional privacy right in a western sense. Students learned that constitutional and legal norms were different. Legal norms had direct effect, so they could be realized by an application to a set of facts. Constitutional norms were realized through application of a statute. The statute projected them into legal norms, which would be of direct effect.[17]

---

14. Kuzmik, *supra* note 12, at 611.

15. A. ARZHANOV ET AL., TEORIJA GOSUDARSTVA I PRAVA [THEORY OF STATE AND LAW] 494 (1949) (author's trans.) (on file with author).

16. KONSTITUTSIIA SSSR (1977) [Konst. SSSR] [USSR Constitution] art. 56 (U.S. Dep't of Commerce, Office of General Counsel trans., 1995) [hereinafter USSR CONST.].

17. *See, e.g.*, S.I. RUSINOVA & V.A. R'ANZHIN, SOVETSKOJE KONSTITUTSIONNOJE PRAVO [SOVIET CONSTITUTIONAL LAW] 16–17 (1975) (author's trans.) (on file with author).

Judges were not allowed to interpret constitutional norms directly in litigation; this could lead to a lack of uniform application. Textbooks taught:

> [The] [p]olitical system of the Soviet society does not know such source of law as judicial precedence, which so easily leads to deviations from the foundations of legality and undermines the role of representative bodies of the state in legislative activity. In the Soviet State, the judicial bodies realize justice as one of the forms of application of law not connected with lawmaking.[18]

Similarly, unlike in the EU and the United States, concern about data protection was not stirred by a popular use of technology. Prior to independence, home telephones and computers were scarce. Upon independence, Ukraine inherited an antiquated phone system, with less than five percent of the rural population having access to home telephones,[19] and more than 3.5 million applications for telephone installation outstanding for years.[20]

Moreover, there were no private parties to misuse personal information. The word "private" itself was taboo. Even the Civil Code, the last bastion of quasi-private law, which was needed to govern "property-related and connected non-property-related relations for creation of material and technical foundation for communism,"[21] openly despised the term "private." The Code recognized citizens' rights to possess, use, and dispose of certain items at their discretion.[22] However, this was considered personal, rather than private property. In a centralized, planned economy there were no private businesses to take people's personal information and use it for their own purposes. There were no private journalists to pry into people's personal lives to earn some dirty money; all business and media were state-owned.

Finally, the notion of individuals having private information was contrary to Soviet communist ideology. The preamble to the USSR Constitution established that "[t]he law of life is the care of all about the

---

18. S.N. BRATUS' & I.S. SAMOSCHENKO, OBSCHAJA TEORIJA SOVETSKOGO PRAVA [GENERAL THEORY OF THE SOVIET LAW] 136 (1966) (author's trans.) (on file with author).

19. U.N. DEV. PROGRAMME (UNDP), 9 UNDP REPORT, E-READINESS ASSESSMENT OF UKRAINE 2002 [hereinafter UNDP REPORT].

20. CENT. INTELLIGENCE AGENCY (CIA), THE WORLD FACTBOOK 561 (2005).

21. Tsyvil'nyj Kodeks URSR [Civil Code of the Ukrainian Soviet Socialist Republic] (1963) art. 1 (author's trans.) (on file with author) [hereinafter Ukr. Civ. Code].

22. *Id.* art. 88 (repealed by Law No. 3718-12 of Dec. 16, 1993).

welfare of each, and the care of each about the welfare of all."[23] Under this principle, no members of society had to hide anything from others. It was admitted that irresponsible individuals could gossip and distort personality profiles and newspapers, which would create mistakes in interpreting the facts. For such occurrences the civil code provided an article on defamation, which required the publishers to retract and rectify incorrect data.[24] In addition, the criminal code threatened prosecution for libel[25] and insult.[26]

Implementing legal regimes to protect personal data from private controllers was not a goal of the Soviet Ukraine. However, upon attaining independence in 1991, the political winds changed and the protection of privacy became a hot issue.

B. After the Fall of the Soviet Union

When Ukraine became independent, several developments turned privacy rights and private data controllers into hot issues. These developments included liberalized conditions for private collection of personal data, a switch to a western-style human rights protection approach, and initiation of a course toward integrating into the European community.

The reforms made it economically and technologically possible for private actors to collect personal data. Soon after proclaiming independence, Ukraine adopted a series of laws on capitalization and privatization of the economy. For example, in 1991 it promulgated the Law on Property,[27] Law on Enterprises,[28] and Law on Business Associations.[29] These instruments restored the concept of private property in mainstream legal use and created a framework for the development of private businesses. In 1992, the Law on Information[30] liberalized information flows. This law provided that "all citizens of Ukraine,

23. USSR CONST. pmbl.

24. Ukr. Civ. Code art. 7.

25. Kryminal'nyj Kodeks URSR [Criminal Code of Soviet Ukraine] #2001-V, art. 125 (Dec. 28, 1960) (author's trans.) (on file with author).

26. *Id*. art. 126.

27. Zakon Ukrajiny pro Vlasnist [Law of Ukraine on Property], #697–XII (Feb. 7, 1991) (author's trans.) (on file with author).

28. Zakon Ukrajiny pro Pidpryjemstva [Law of Ukraine on Enterprises], #887-XII (Mar. 27, 1991) (author's trans.) (on file with author).

29. Zakon Ukrajiny pro Hospodars'ki Tovarystvai [Law of Ukraine on Business Organizations], #1576-XII (Sept. 19, 1991) (author's trans.) (on file with author).

30. Zakon Ukrajiny pro Informatsiju [Law of Ukraine on Information] #2657-XII (Oct. 2, 1992) (author's trans.) (on file with author) [hereinafter Law on Information].

juridical persons, and state agencies have the right to information, which denotes the ability to freely acquire, use, spread, and store information."[31] The subsequent Law on the Press,[32] Law on Television and Radio-broadcasting,[33] and Law on Information Agencies[34] established baselines for the functioning of private media. By 2001, almost eighty percent of the newspapers and a majority of telecommunication stations were privately owned.[35] In addition, the legal system closely addressed the issue of technology development. The 1998 national concept of "informatization" endorsed "creation, development, and utilization of information technologies [for the purposes] of . . . further democratization . . . and facilitation of equitable integration of Ukraine into the international community."[36]

The existing infrastructure for technology development still substantially lags behind that of the EU and the United States. However, the recent United Nations Development Programme's (UNDP) *E-Readiness Assessment for Ukraine* has indicated that Ukraine's potential is immense.[37] With its 15,000 annual graduates who have information technology as a component of their university studies,[38] Ukraine has been fourth in the world in the number of certified information technology professionals.[39] In 2001, an estimated 370,000 to 400,000 personal computers were sold in the Ukrainian market,[40] representing an annual

31. *Id.* art. 9.

32. Zakon Ukraijiny pro Drukovani Zasoby Masovoji Informatsiji (Presu) v Ukrajini [Law of Ukraine on Printed Media in Ukraine] #2782-XII (Nov. 16, 1992) (author's trans.) (on file with author).

33. Zakon Ukrajiny pro Telebachenn'a I Radiomovlenn'a [Law of Ukraine on Television and Radio-Broadcasting] #3759-XII (Dec. 21, 1993) (author's trans.) (on file with author).

34. Zakon Ukrajiny pro Informatsijni Ahenstva [Law of Ukraine on Information Agencies] #74/95-BP (Feb. 28, 1995) (author's trans.) (on file with author). *See also* J.A. FLEJSHITS, LICHNYJE PRAVA V GRAZHDANSKAM PRAVE SOJUZA SSRI KAPITALICHESKIH STRAN [PERSONAL RIGHTS IN CIVIL LAW OF THE USSR AND CAPITALISTIC STATES] 101 (Yurizdat NKYu USSR 1941) (author's trans.) (on file with author).

35. KHARKIV HUMAN RIGHTS GROUP (KHRG), OHL'AD POVIDOMLEN' PRO KONFLIKTY V INFORMATSIJNIJ SFERI [OVERVIEW OF PUBLICATIONS ABOUT CONFLICTS IN THE SPHERE OF INFORMATION] (Kharkiv 2001) (author's trans.) (on file with author); 2 SVOBODA VYRAZHENN'A POHL'ADIV [FREEDOM OF EXPRESSION OF VIEWS] 24(65) (2002); quoting 58 NARODNA ARMIJA 3 (Mar. 28, 2001)) [hereinafter KHRG] (author's trans.) (on file with author).

36. Zakon Ukrajiny pro Kontseptsiju Natsional'noji Prohramy Informatyzatsiji [Law of Ukraine on Concept of National Program of Informatization] #75/98-BP (Feb. 4, 1998) (author's trans.) (on file with author).

37. UNDP REPORT, *supra* note 19, at intro.

38. *Id.* at 36.

39. Emmy B. Gengler, *Ukraine and Success Criteria for the Software Exports Industry*, 13 EC. J. INFO. SYS. DEV. COUNTRIES, 8, 9 (2003), *available at* http://new.ejisdc.org/ojs/include/getdoc.php?id=82&article=93&mode=pdf.

40. UNDP REPORT, *supra* note 19, at 39.

growth rate of seventeen to twenty-two percent.[41] The mobile (cellular) phone market has experienced unprecedented growth of just under 200 percent a year, acquiring two and a half million users by 2002.[42] The market for Internet Service Providers (ISPs) became unlicensed, expanding from 100 providers in 1997 to more than 300 by 2002.[43] The number of Internet users has grown from only 400 people in 1993 to 900,000 people in 2002.[44]

This technological growth has had pros and cons. Economic and technological developments made it possible for private actors to acquire wide access to personal data. However, the government instantaneously acquired an obligation to regulate such access, because promotion of western-style protection of human rights in Ukraine, including the right to privacy, became a high priority of the government after independence.

It should be noted that Ukraine originally incorporated a human rights agenda into its lawmaking before independence. In 1990, the *Verkhovna Rada* (National Legislature) promulgated the Declaration of Sovereignty, which expressed the nation's will to create a state-based rule of law with comprehensive safeguards for human rights and freedoms.[45] In 1996, Ukraine's new Constitution expanded this aspiration, providing that: "the human being, his or her life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value. Human rights and freedoms and their guarantees determine the essence and orientation of the activity of the State."[46]

Article 23 of the new Constitution offers general recognition of the right of privacy by stipulating that "every person has the right to free development of his or her personality. . . ."[47] Article 31 protects the privacy of mail, telephone conversations, telegraph, and other correspondence.[48] Article 32 outlaws interference with personal and family life; forbids the collection, storage, use, and dissemination of confidential information about a person without his or her consent; and entitles individuals to examine information collected about them, as well as rectify

41. *Id.*
42. *Id.* at 10.
43. *Id.* at 14.
44. U.N.S. Div., Millenium Indicators: Country Profiles, *at* http://unstats.un.org/unsd/mi/mi.asp? (last visited Jan. 5, 2006).
45. Deklaratsija pro Derzhavnyj Suverenitet Ukrajiny [Declaration on the Sovereignty of Ukraine] #55-XII (July 16, 1990) (author's trans.) (on file with author).
46. UKR. CONST. art. 3.
47. *Id.* art. 23.
48. *Id.* art. 31.

incorrect information or demand its expulsion.[49] Unlike the USSR Constitution, the Constitution of Ukraine was adopted as a piece of directly enforceable law.[50] The Ukraine Constitution proclaims an individual's right to appeal any constitutional violation in a national court before the National Human Rights Commissioner.[51] The Constitution further states that upon exhaustion of all domestic remedies, an individual may seek protection from the international community.[52]

In addition to internal economic and political developments demanding that the State ensure data protection against misuse by private controllers, Ukraine adopted several international obligations urging the government to shape the local data protection framework within the course of global standards.

Ukraine has articulated a desire to integrate into the European Union. Presidential *Ukaz* (Edict) # 615/98 of June 11, 1998 endorsed the strategy of integration. This strategy established priorities such as the harmonization of human rights frameworks and legislation on information and communications technologies.[53] In 1997, Ukraine ratified the European Convention of Human Rights (ECHR) and recognized the jurisdiction of the European Court of Human Rights over its territory.[54] New social and political conditions required the national legal system to address privacy of personal data as an ultimate concern.

C. Current Mechanisms for "Controlling" Private Controllers in Ukraine: Why Long for a New Statute?

In order to fulfill its new data protection obligations, Ukraine has taken a number of legislative steps. The first mention of the term "personal data" predates the Constitution and traces back to the 1992 Law on Information.[55] Article 23 of this law defined the basic term "personal data" (*personal'ni dani*) as information regarding "nationality, education, family

49. *Id.* art. 32.
50. *Id.* art. 8.
51. *Id.*
52. *Id.* art. 55.
53. Ukaz Presidenta Ukrainy [Edict of the President of Ukraine] #615/98 (June 11, 1998) "*On Strategy of Integration into the European Union*," § 1, *available at* http://ukraine-eu.mfa.gov.ua/eu/en/publication/content/1992.htm (last visited Jan. 5, 2006).
54. Zakon Ukrajiny pro Ratyfikatsiju Konventsiji pro Zakhyst Prav i Osnovnykh Svobod L'udyny 1950, Pershoho Protocolu i Protocoliv # 2, 4, 7 ta 11 do Konventsiju [Law of Ukraine on Ratification of Convention on Protection of Human Rights and Fundamental Freedoms of 1950, of First Protocol and Protocols # 2, 4, 7, and 11 to the Convention] #475/97-BP (July 17, 1997) (author's trans.) (on file with author).
55. Law on Information, *supra* note 30.

status, religious beliefs, health status, as well as address, date and place of birth."[56] It then placed this term within a broader concept of information about a person, which was defined as "entirety of documented or publicly announced notions (information, knowledge) about a person."[57] The Law on Information specifically restricted dissemination of certain categories of sensitive data, such as "information about health (medical secrets), financial deposits, profits from entrepreneurship, adoption, correspondence, telephone conversations and telegraph transmissions."[58] The law also established basic principles of handling information about a person. It bans collection of personal information without the subject's prior consent (except when expressly authorized by the statute).[59] It also urges for collection and storage to be strictly limited and used only for a lawfully established purpose; it restricts third persons from accessing information about another collected by state authorities, organizations, and officials; and it requires all organizations that collect information about citizens to register their respective databases with the state.[60] Under the law, subjects are entitled both to know at the time of collection what information is being collected and for what purpose,[61] and also to access the information collected[62] and check its accuracy, completeness, and relevance.[63] Finally, the law introduced a private civil cause of action for damages inflicted by violation of the data subject's rights.[64]

In addition, the legislature addressed various aspects of handling sensitive personal information, in a variety of instruments that regulate the activities of certain types of private controllers. Some twenty acts contain provisions detailing collection, processing, and transfer of information about physical persons in various contexts.[65] These include the Law on Notary,[66] Law on Professional Advocacy,[67] Law on Communication,[68]

56. *Id.* art. 23.
57. *Id.*
58. *Id.* art. 46.
59. *Id.* art. 23.
60. *Id.* art. 31.
61. *Id.*
62. *Id.* art. 23.
63. *Id.* art. 31.
64. *Id.* arts. 31, 44, 47, 49.
65. ALEXANDER A. BARANOV ET AL., PRAVA CHELOVEKA I ZASCHITA PERSONAL'NYKH DANNYKH [HUMAN RIGHTS AND PROTECTION OF PERSONAL DATA] 67 (2000) (author's trans.) (on file with author).
66. Zakon Ukrajiny pro Notariat [Law of Ukraine on Notary], # 3425-XII (Sept. 2, 1993) (author's trans.) (on file with author).
67. Zakon Ukrajiny pro Advokaturu [Law of Ukraine on Professional Advocacy], #2887-XII (Dec. 19, 1992) (author's trans.) (on file with author).

Law on Militia,[69] Law on Banks and Banking Activity,[70] Law on Protection of Information in Automated Systems,[71] and Law on Prevention of the Spread of AIDS and Social Protection of the Population.[72]

Finally, the newly adopted Civil Code, which entered into force on January 1, 2004,[73] provided a number of tools applicable to any context and allowed individuals to take steps to protect their private data against tortious harm.[74] The Code provides redress for subjects of data collection in two ways. First, it explicitly secures a number of sectoral privacy-related safeguards. Second, it enables an individual to assert and claim a violation of a personality (personal, non-property-related) right not enumerated in the Code.[75] The sectoral safeguards provided by the Code include a right to privacy of one's health status,[76] personal life,[77] personal papers,[78] correspondence,[79] and inviolability of business reputation.[80] It enables individuals to control publicity of their image in photos, artistic pieces, and films.[81] It pays special attention to the inviolability of one's personal name.[82]

Complementary to these aspectual safeguards, the Code allows much individual discretion in defining the content and scope of other rights relating to personal data. It establishes that the list of personality rights is non-exhaustive. As such, the Code offers general guidance, but does not provide an enumerated list of what constitutes a personality right. Pursuant

---

68. Zakon Ukrajiny pro Zv'jazok [Law of Ukraine on Communication] #160/95-BP (May 16, 1995) (author's trans.) (on file with author).

69. Zakon Ukrajiny pro Militsiju [Law of Ukraine on Militia] #565-XII (Dec. 20, 1990) (author's trans.) (on file with author).

70. Zakon Ukrajiny pro Banky i Bankivs'ku Dijal'nist' [Law of Ukraine on Banks and Banking Activity] # 872-XII (Mar. 20, 1991) (author's trans.) (on file with author).

71. Zakon Ukrajiny pro Zakhyst Informatsiji v Avtomatyzovanykh Systemakh [Law of Ukraine on Protection of Information in Automated Systems] # 80/94-BP (July 5, 1994) (author's trans.) (on file with author). This law primarily governs security standards for automated systems containing protected information and establishes the right of individuals and entities to cooperate with counterparts in other countries in processing, exchange, and trade of open information.

72. Zakon Ukrajiny pro Zapobihann'a Poshyrenn'u Zakhvor'uvann'a na SNID ta Sotsial'nyj Zakhyst Naselenn'a [Law of Ukraine on Prevention of the Spread of AIDS and Social Protection of the Population] (Dec. 12, 1991) (author's trans.) (on file with author).

73. *See generally* Ukr. Civ. Code, *supra* note 21.

74. *Id.*

75. *Id.* art. 286.

76. *Id.* art. 301.

77. *Id.* art. 303.

78. *Id.* art. 306.

79. *Id.* art. 299.

80. *Id.* arts. 307–308.

81. *Id.* arts. 294–296.

82. *Id.* art. 270.

to article 269, personality rights are rights that (1) belong to each individual from birth or pursuant to the law, (2) do not have economic content, and (3) are so closely connected to the physical persons that their subjects may not voluntarily renounce them.[83] Under the concept of personality rights, the new Civil Code enabled individuals to challenge actions of others based on so-called customized concepts.[84]

In spite of the fact that a variety of legislative acts address data protection in this new setting, Ukrainian policymakers remain unsatisfied with the existing framework. European integration has brought with it the idea that a new comprehensive, uniform bill on data protection is needed to address the issue in its entirety. To this effect, the *Verkhovna Rada* has registered two bills: the Bill on Personal Character Information and the Bill on Protection of Personal Data.[85] This second bill passed in its first reading on May 15, 2003.

Overall, having completed a number of steps to ensure data protection in recent years, Ukraine is looking to take another step, opening a new era in treating the subject. A new comprehensive law on data protection is expected, in regards to dealing with private controllers, to clarify three intertwined but distinctly important issues. First, where does data protection belong in the macrostructure of other institutes of the legal system? Second, what should be the microstructure of definitions, principles, and rules of law? And finally, how should the interest in data protection correlate to the equally important interest in ensuring free information flows in a democratic society?

In terms of the macrostructure, the statute is expected to enhance the public-law component of the data protection law and secure governmental enforcement and oversight. The euphoria regarding human rights in the 1990s produced two opposing trends in approaching human rights enforcement. On the one hand, it inspired the creation of an entirely new chapter on personality rights in the 2004 Civil Code.[86] Dr. Dovhert, a co-author of the Code, wrote, "[n]orms that foster development of an individual as a personality must precede norms that foster her formation as an owner of property or a party to a contract."[87] Lawmakers agreed that

83. *Id.* art. 269.

84. *See generally id.*

85. Pro Informatsiju Personalinaho Harakteru [Bill on Personal Character Information] #2016 of July 22, 2002; both bills are available at http://ilaw.org.ua/list_bill.php (last visited Jan. 5, 2006).

86. Ukr. Civ. Code, at bk. II.

87. A. DOVHERT, KODYFIKATSIJA PRYVATNOHO (TSYVIL'NOHO) PRAVA UKRAJINY [CODIFICATION OF PRIVATE (CIVIL) LAW OF UKRAINE] 156 (2000) (author's trans.) (on file with author).

predominantly Soviet-style public enforcement of constitutional rights was not sufficient. Administrative protection is restricted to violations of rights by the administrative bodies. Criminal liability depends upon the degree of guilt; the idea is to correct a violator by means of repression. Concern about restitution of the victim's peace of mind, which has been ruined by the committed violation, is foreign to the criminal law. Meanwhile, due protection of personal rights requires safeguarding them from any infringement, regardless of who commits the infringement and whether she is at fault.[88]

On the other hand, scholars opposed to introducing the concept of individual rights into the Civil Code have expressed a fear that private action may diminish or distort the constitutional meaning of fundamental rights. Dr. Znamenskij, for example, emphasized that the pathos of international human rights standards is in the hands of the state to protect.[89] He theorized that the state may get too comfortable encouraging private enforcement and detach itself from an obligation to prosecute human rights violations by public means.[90] With public enforcement (criminal and administrative), the state would share the victim's burden for evidence collection. Moreover, public enforcement would condemn a violation on behalf of the entire nation and would demonstrate the violation's incompatibility with the values of the society.[91]

The current data protection framework provides baseline regulations for the conduct of private controllers and offers data subjects the ability to enforce the regulations through contractual clauses and tort litigation. However, if a controller does not comply with legal requirements or the demands of the subject, there is little public oversight capable of intervening on the subject's behalf unless the subject takes private action.

If data protection is a fundamental human right guaranteed by the Constitution, is it enough that the state provides only private enforcement? Would not the state run afoul of its constitutional obligation, allowing violations to happen if an individual, out of ignorance, business, or intimidation, refused to take a stand and go to court? To address these

88. Such reasoning was articulated by some Soviet scholars as early as 1940s, but it was disfavored. *See, e.g.*, FLEJSHITS, *supra* note 34.

89. *See* Georgiy Znamenskyy, *Khyby Knyhy II Proektu Tsivil'noho Kodeksu Ukrajiny* [*Shortcomings of Book II of the Draft Civil Code of Ukraine*], 3 UKRAJINS'KE PRAVO [UKRAINIAN LAW] 122–15 (1997) (author's trans.) (on file with author).

90. *See id.*

91. O.A. KRASAVCHIKOV, 1 SOVETSKOJE GRAZHDANSKOJE PRAVO [SOVIET CIVIL LAW] 423 (1972) (author's trans.) (on file with author).

fears, the Bill on the Protection of Personal Data envisions specialized National Data Protection Authorities (DPAs).[92]

Another problem that the law is expected to address is the poor microstructure of the data protection institute, specifically the lack of organized rules and streamlined definitions. Because adoption of information-related legislation over the last ten years has been patchy and haphazard, there is a growing annoyance with terminological ambiguities and incongruity between rules. For example, analysts Bagraj and Kravtsov note that, while procedural aspects of the law are described in detail, the system of definitions is insufficiently developed and confusing.[93] For instance, in some acts the term *informatsija* (information) itself is defined through the term *svedenija* (to know).[94] Other acts instead define it through the term *dani* (data).[95] A statute on data protection is seen as the fastest and most appropriate way to remove ambiguities by offering clear-cut definitions of such baseline terms as "personal data," "data controller," "filing system," and "data processing."

Another challenge of the current data protection system is finding a way to make modifications to the system without interrupting the flow of information. Article 23 of the Ukrainian Constitution establishes a general balancing principle that "[e]very person has the right to free development of his or her personality if the rights and freedoms of other persons are not violated thereby."[96] Further, article 32 of the Constitution bans "[t]he collection, storage, use and dissemination of confidential information about a person without . . . consent," but at the same time provides an exception "in the interests of national security, economic welfare, and human rights."[97] Likewise, article 34, which secures the right to freedom of speech, explains that "everyone has the right to freely collect, store, use, and disseminate information."[98] It imposes an immediate restriction in the

92. Proekt Zakonu Ukrajiny pro Zakhyst Personal'nykh Danykh [Draft Law of Ukraine on Protection of Personal Data] #2618 of Jan. 10, 2003, art. 3 (author's trans.) (on file with author) [hereinafter Bill on Data Protection].

93. V.V. Bagraj & H.A., Kravtsov, Analiz Zakonodatel'noj Bazy Ukraijiny v Sfere Zaschity Informatsiji [Analysis of the Legislative Framework of Ukraine in the Sphere of Protection of Information] 9, *available at* http://gipi.internews.ua/ukr/Public_ICT/Analitics/Obsor_LawArticle.doc (last visited Jan. 24, 2006) (author's trans.).

94. *Id.* at 5. This term is from the Slavic term *vedat*.

95. *Id.* It is unclear how all these terms correlate with each other.

96. UKR. CONST. art. 23.

97. *Id.* art. 32.

98. *Id.* art 34.

interest of "[protecting] the reputation or rights of other persons" and "preventing the publication of information received confidentially . . . ."[99]

The Soviet legacy may make Ukrainian courts reluctant to shape policy by fairly balancing and filling the gaps of the existing legislation. The tradition of looking to the legislature to define the precise scope of legal rights and duties is historically rooted. This is reflected, for instance, in the Constitutional Court's 1997 ruling on the issue of data collection. In this ruling the Court, authorized to provide official interpretation of statutes and invalidate unconstitutional statutory provisions, reflected its deep frustration with statutory loopholes in the absence of clearly defined statutory language. The Court regretted that the statutory framework concerning information flow contains unclearly defined, colliding provisions and loopholes, which negatively affects enforcement of constitutional rights and freedoms of a human and a citizen[,] the law does not completely define the rules for collection, storage, utilization and dissemination of information."[100]

Under these conditions, a new statute is expected to prevent possible confusion among controllers, enforcement, and judges, ensuring uniformity in the application of concurring constitutional principles. Will the expectations of the Ukrainian policymakers come true? Is a new statute truly necessary? Will it advance the system of data protection? Within thirteen years of its independence, Ukraine has achieved amazing success in the setting of a framework for data protection. The need to create this framework, which took decades to evolve in western Europe and the United States, bypassed Ukraine until the 1990s. The country was busy building a society in which data protection law was believed to be unnecessary. As Ukraine is standing at a fork in the "decision-making road," assessing the "pros" and "cons" of an omnibus statute, the next Part explores the existing data protection frameworks in the EU (with its comprehensive statutory protection) and the United States (with its market self-regulation and sectoral statutes). What is it the omnibus statute has given to Europeans that Americans do not have? And what do Americans gain by avoiding a comprehensive statute?

III. TO HAVE OR NOT TO HAVE: WHAT ARE THE OPTIONS?

In the late eighteenth century, the U.S. Constitution was inspired by the Enlightenment, embracing the idea that the state is a product of a social

99. *Id.*
100. *In re* Ustymenko, Opinion No. 18/203-97 (Ukr. Const. Ct. 1997).

contract. It was suggested that negative rights restricting the state from interfering with private affairs were the basis and foundation for freedom and pursuit of happiness. One such negative right, freedom of expression, was thought to be a watchdog of governmental accountability. In response to World War II, the 1950 European Convention of Human Rights (ECHR) was drafted. Through the ECHR, Europeans declared a longing to restore human dignity and the essential right to personal inviolability.[101] How did the two philosophies affect data protection frameworks in terms of their micro and macro structures, and in terms of balancing with the free flow of information?

A. General Overview of the EU and U.S. Data Protection Frameworks

1. Data Protection in the EU

The European framework for data protection is comprised of a whole orchestra of directives and recommendations of the European Union authorities, intertwined with data protection legislations of the member states. However, this orchestra follows its prime conductor, a single statutory instrument, the General Directive of the European Commission and the Council.

The principle of subsidiarity, a fundamental concept of EU legislation, mandates that matters be solved at the lowest possible level.[102] It also provides member states with significant discretion in setting national data protection frameworks. Inspired by the European Convention on Human Rights, many member states enacted laws on data protection by 2000.[103] Until recently, these laws differed considerably in structure, content, and approach.[104] In spite of these variations, one can obtain a basic sense of how European data protection works through the study of the EU directives. The unique legal force of the directives gives them a special leading role in shaping the national law of member states. Directives bind member states, but only in regards to the results, leaving the processes and systems of implementation considerably up to national authorities.[105]

---

101. *See, e.g.*, Marsha C. Huie et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 428 (2002).

102. Treaty Establishing the European Community, Nov. 10, 1997, 1997 O.J. (C 340) 3, art. 5 (consolidated version, art. 5, Dec. 24, 2002, O.J. (C 325)) [hereinafter EC Treaty].

103. European Commission, *Status or Implementation of Directive 95/46 or the Protection of Individuals with Regent to the Processing of Personal Data*, http://europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.html (last visited Jan. 5, 2005) [hereinafter *Commission Report*].

104. CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 13 (2003).

105. GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN UNION LAW 76 (2002).

However, should a government fail to implement a directive promptly and properly, its nationals are entitled to refer directly to the directive and assert violation of their rights in court.[106]

Several directives address data protection issues in the European Union. For example, the Directive on Privacy and Electronic Communications governs data protection in telecommunications, faxes, e-mail, the Internet, and other similar services.[107] Basic rules applicable to online advertising have been harmonized through the Distance Selling[108] and the E-Commerce Directives.[109] The EU Electronic Signatures Directive[110] contains data protection rules for providing electronic signature services. However, all of these tools were adopted to supplement and solidify another comprehensive statutory instrument, the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Directive).[111] It was adopted in 1995 to harmonize the divergent legislation of the member states by setting fundamental guidelines for both the public and private sectors,[112] and, in a way, has become a constitution of European data protection.

2. Data Protection in the United States

U.S. data protection (or information privacy) law does not center around a single statute. It is better described as "an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law."[113]

---

106. *Id.* at 76–80.

107. Council Directive 2002/58, Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC), *available at* http://europa.euint/eur-lex/pri/en/oj/dat/2002/1_201/1_2012002073/en00370047.pdf.

108. Council Directive 97/7, Directive on the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19 (EC), *available at* http://europa.eu.int/comm/consumers/policy/developments/dis_sell/dist01_en.pdf.

109. Council Directive 2001/31, Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market, 2000 O.J. (L 178) (EC), *available at* http://europa.eu.int/eur-lex/pri/em/oj/dat/2000(1.178/1.17820000717en00010016.pdf.

110. Council Directive 1999/93, Directive on a Community Framework for Electronic Signatures, 1999 O.J. (L 13) 12 (EC), *available at* http://europa.evint/eur-lex/pri/en/oj/dat/2000/1.013/1.01320000119en00120020.pdf.

111. Council Directive 95/146, Directive on the Protection of Individuals with Regent to the Processing of Personal Data and on the Free Movement of Such Data 1995 O.J. (L 281) 31 [hereinafter General Directive]. *See also* KUNER, *supra* note 104, at 17.

112. *Id.*

113. SOLOVE & ROTENBERG, *supra* note 11, at 2.

Unlike the European Convention, the U.S. Constitution does not specifically mention privacy. Nevertheless, inspired by social demand for legal protection of the ability "to be let alone,"[114] the Supreme Court found that the Constitution has certain "penumbras" or "zones of privacy."[115] For example, the First Amendment guards freedom of speech and at the same time secures a private right to speak anonymously. The Third Amendment protects the privacy of the home by preventing the government from allowing soldiers to reside in people's homes. The Fourth Amendment provides that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[116]

Because there is no single constitutionally or statutorily defined right to privacy, non-governmental actors have considerable discretion in establishing or not establishing data protection practices. However, even in the absence of a statute, since the 1890 Warren and Brandeis article *The Right to Privacy*,[117] U.S. courts have entertained actions for intrusions into the privacy of individuals. The common law practice has established four distinct "privacy torts": "(1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[118]

Toward the middle of the twentieth century, when technological advances allowed for unprecedented collection of personal information in databases, data protection became a defining social issue for American society.[119] However, faithful to the approach of economy of state action, the legislature responded by creating privacy rights only in specific contexts. For instance, the Children's Online Privacy Protection Act (COPPA) restricted collection of personal data from children.[120] The Gramm-Leach-Bliley Act (GLB) required financial institutions to disclose their privacy policies and practices to consumers.[121] The Health Insurance

114. The formulation of intuition about privacy as a right "to be let alone," usually attributed to and extensively used by Samuel Warren and Louis Brandeis in their article, traces back to earlier authors. Warren and Brandeis actually borrowed the quote from Thomas C. Cooley's, *Law of Torts* (1880). For a correct citation see William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

115. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

116. *Id.*

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

118. Prosser, *supra* note 114, at 389.

119. SOLOVE & ROTENBERG, *supra* note 11, at 22.

120. SOLOVE & ROTENBERG, *supra* note 11, at 561. *See also* Children's Online Privacy Protection Act, 15 U.S.C. § 650 et. seq. (1998).

121. SOLOVE & ROTENBERG, *supra* note 11, at 534. *See also* Gramm-Leach-Bliley Act, 15 U.S.C.

Portability and Accountability Act (HIPAA) protects privacy of medical records.[122] Apart from this "piecemeal legislation," U.S. law "does not recognize any general right to control the collection and use of personal information."[123]

Which approach would be more appropriate for Ukraine, the European comprehensive statutory model or U.S. style self-regulation? Each framework presents valuable considerations.

B. Macro-Structure of the Western Data Protection: A Fundamental Human Right or a Valuable Private Asset?

In terms of the macro-structure, the need for a statute is predicated on a central question: how private is the right to information privacy? If it is a fundamental human right, the government may be able to justify a mandate to establish prophylactic statutory restrictions on private data controllers to prevent any abuse of the public value. On the other hand, if it is a private asset, prophylactic governmental interference in a democratic society may be excessive, and the government should abstain from regulation except, perhaps, to create a general private-law framework for fair dealings in contracts and fair compensation in torts.

1. The Human Rights Approach and the Need for Public Enforcement

From its very inception, EU culture has treasured privacy of personal data. Some commentators even compare the EU attitude towards personal information to the reverence for the integrity of the human body: no economic considerations can make a civilized legal system approve sale of human legs, arms, or heads.[124] The current EU legal system derives from the European Economic Community (EEC), an organization established in 1957 to advance four largely economic freedoms: the free movement of goods, people, services, and capital throughout the member states.[125] The founding treaties conferred no legislative powers in the sphere of human

---

§ 6801, et seq. (1999).

122. SOLOVE & ROTENBERG, *supra* note 11, at 210. *See also* Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 300gg and 29 U.S.C. § 1181 et seq. (1996). While in many ways HIPAA protects privacy of medical records, it also includes many provisions that weaken privacy protection of such records.

123. RONALD J. MANN & JANE K. WINN, ELECTRONIC COMMERCE 129 (2002).

124. Lynn Kramer, Comment, *Private Eyes Are Watching You: Consumer Online Privacy Protection-Lessons from Home and Abroad*, 37 TEX. INT'L L.J. 387, 390 (2002).

125. EC Treaty, *supra* note 102, art. 3, § 1(c).

rights to the centralized bodies.[126] However, with the evolution of the EEC into the Union, the human rights focus has become increasingly connected to all legal developments. The proposed EU Constitution states that that the European Union "[draws] inspiration from the cultural, religious, and humanist inheritance of Europe, the values of which . . . have embedded within the life of society the central role of the human person and his or her inviolable and inalienable rights. . . ."[127]

It is notable that the *Stauder* case in 1969,[128] the first case ever to raise human rights issues at the EEC level, was a data protection case. Stauder, an impoverished German national, contested the requirement that he identify himself in order to obtain coupons allowing him to purchase butter at a reduced fee. The European Court of Justice took this factually small but symbolically vital case seriously, ruling that "the Community's measures should be set aside if they fall short to respect a fundamental human right."[129]

The human rights approach to the treatment of personal data justified creation of the General Directive as a central source for the EU law on information privacy. The Directive seeks to "protect the fundamental [right] of natural persons . . . to privacy with respect to the processing of personal data."[130] In accordance with the human rights approach, the government can restrict data flows *a priori*, whether the data subjects ask for the protection or not.[131] As Reidenberg observes, the European vision of governance "generally regards the state as the necessary player to frame the social community in which individuals develop and in which information practices must serve individual identity. . . . Law thus enshrines prophylactic protection through comprehensive rights and responsibilities. Indeed, citizens trust government more than the private sector with personal information."[132]

---

126. GEORGE BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN UNION LAW 256 (2002)

127. The European Convention, Draft Treaty Establishing a Constitution for Europe, July 18, 2003, 820 Eur. Conv. 1. EU member states have set November 2006 as the deadline for ratification of the EU Constitution, and it is currently being considered for possible ratification by EU member states. Spain was the first member state to hold a national referendum on the EU Constitution, approving it in February 2005. "If fewer than twenty-five member states sign the EU Constitution, the proposed draft will undergo formal revisions." *French to Vote in May*, N.Y. TIMES, Mar. 5, 2005, at A5. As of November 24, 2005, twelve EU member states had ratified the treaty. *EU Constitution: Where Members Stand*, BBC NEWS.COM, Nov. 25, 2005, http://news.bbc.co.uk/2/hi/europe/3954327.stm (last visited Jan. 24, 2006).

128. Case 29/69, Erich Stauder v. City of Ulm, Sozialent, 1969 E.C.R. 419.

129. *Id.*

130. General Directive, *supra* note 111, art. 1, § 1.

131. Kramer, *supra* note 124, at 407.

132. Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 731

Under the General Directive, private and governmental processors and controllers are bound equally.[133] Because data protection is a fundamental human right, the European model proposes to regulate it under a horizontal-action doctrine. This doctrine, inspired by the German concept of *drittwirkung* (horizontal action), suggests that the Constitution governs not only relations between individuals and the state, but also relations between private individuals. The state is obligated not only to abstain from encroaching upon human rights to thus foster their effective realization through relevant conditions, but also to provide for their observance by private persons.[134]

The burden of compliance imposed on private controllers by the statute triggers a question: do the protected data subjects appreciate what the law does for them? A 2002 European Commission's Open Consultation survey of 9,156 European citizens yielded an interesting result: while in theory a number of respondents are concerned about data protection, in practice they rarely take steps to exercise the rights provided by the EU legislation.[135] For instance, sixty-nine percent of the respondents named fear of data misuse as a main reason to limit their online transactions, yet only twenty-eight percent of the respondents had applied to data controllers to access their personal record.[136] Of those who did apply and received either a negative response or no response from the data controllers, only fifteen percent bothered to lodge a complaint.[137]

These findings are hard to evaluate. An opponent to the European approach might say it misuses lawmaking and supervisory resources of the government to burden businesses, and those businesses then pass the costs of compliance on to consumers who cannot afford to bear these costs. In contrast, a supporter of this approach may find that the survey illustrates how citizens are unable to protect themselves against invasions of privacy. As Daniel Solove contends,

---

(2001).

133. *See generally* General Directive, *supra* note 111.

134. PRIVACY Ukraine, Prava L'udyny la Internet [Human Rights and the Internet], *available at* http://www.internetrights.org.ua/index.php?page=chapters&id=16 (author's trans.) (last visited Jan. 6, 2006). *See, e.g.*, O.A. Krasavchikov, *supra* note 91, at 423.

135. *Id.* at 219–20.

136. *Id.*

137. European Commission, *Your Views on Data Protection: Questionnaire for on the Implementation of the Data Protection Directive (95/46/EC)*, *available at* http://www.privacyexchange.org/survey/surveys/consultation-citizens.pdf (last visited Dec. 22, 2005) (showing results of on-line consultation from June 20, 2002 to Sept. 15, 2002).

> [i]t is difficult for the individual to adequately value specific pieces of personal information. . . . [because it] is linked to uncertain future uses . . . . An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information. It is the totality of information about a person and how it is used that poses the greatest threat to privacy.[138]

Interestingly, in another survey, the European private data controllers supported governmental control. Thus, ninety-nine percent of respondents agreed that the data protection law was necessary, sixty-four percent found it necessary in all sectors of activity without exception, and fifty-eight percent described the existing regulations as "not unduly strict."[139]

2. The Valuable Asset Approach and Justification for Self-Regulation

The U.S. system, in contrast to that of the EU, has seen the essential value in restricting governmental intrusion into the practices of private data controllers. As Eugene Volokh notes, "[o]nce people grow to accept and even like government restrictions on supposedly 'unfair' communication . . . it may become much easier to accept 'codes of fair reporting,' . . . 'codes of fair debate,' 'codes of fair political criticism,' and the like."[140]

If individuals do not value their personal data enough to actively protect themselves, why should the government bother to do it for them? If personal data is a private asset, then governmental intrusion into regulation of the data flow should be minimal. As Richard Posner notes, "few people want to be let alone. Rather, they want to manipulate the world around them by selective disclosure of facts about themselves . . . . People sell themselves, as well as their goods."[141] If we do not tolerate misrepresentations regarding the quality of goods, why should we tolerate them regarding one's person? Why should the law not promote the free

---

138. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1452 (2001).

139. European Commission, *Flash Eurobarometer: Data Protection in the European Union—Executive Summary*, http://europa.eu.int/comm/public_opinion/flash/fl147_exec_summ.pdf (last visited Oct. 22, 2005) [hereinafter *Eurobarometer*].

140. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1116 (2000).

141. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 233–34 (1981).

flow of information to enable people to make well informed decisions about their relationships?[142]

Flexibility of private law can offer two major regimes for framing data protection: the property (contractual) regime and the liability (tort) regime, each of which has its own advantages.[143]

The liability regime focuses on the harm (damage) that can result from abuse of the data. This was the approach advocated by Warren and Brandeis, the forefathers of privacy rights in the United States.[144] They contended that privacy was different from property, because the core of invasion was mental pain and suffering rather than appropriation of a personal asset.[145] They further contended that publication of a personal occurrence neither deprived a data subject of an asset, nor caused tangible damage, but it did disturb peace of mind.[146] According to Warren and Brandeis, the copyright (intellectual property) concept would not adequately protect personal information either, because it was designed to protect intellectual products, not domestic occurrences.[147]

The liability approach requires governmental interference only in reaction to tangible harm (damage) to a data subject. Typical examples of this approach are *Shibley v. Time*[148] and *Dwyer v. American Express.*[149] In *Shibley*, the court gave no remedy to newspaper subscribers who were unhappy that Time's subscription list was sold to a direct marketing company without their consent. The court saw no actual damage to the subscribers in such a sale.[150] Similarly, in *Dwyer*, the court denied compensation to credit card holders when the company aggregated their spending habits without their knowledge and rented the resulting database to an advertising company.[151] The *Dwyer* court reasoned that although the demographic information was a valuable asset, its collection brought no economic loss to the data subjects. Therefore, its use did not constitute damage to them.[152]

---

142. *See generally* Volokh, *supra* note 140.

143. See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Lawrence Lessig, *The Law of The Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

144. Warren & Brandeis, *supra* note 117.

145. *Id.* at 207.

146. *Id.* at 219–20.

147. *Id.*

148. 341 N.E.2d 337 (Ohio Ct. App. 1975).

149. 652 N.E.2d 1351 (Ill. Ct. App. 1995).

150. *Shibley*, 341 N.E.2d at 339–40.

151. *Dwyer*, 652 N.E.2d at 1351.

152. *Id.* at 1356.

Because the United States developed few restrictions on the types of information that businesses can collect and what they can do with such information,[153] a several billion dollar industry has arisen that is devoted to creating gigantic databases of personal information.[154] Advertisers argue that collection of data permits "them to offer consumers preferred products and services, improve their marketing efficiencies and Website designs, and subsidize free Internet content. . . ."[155]

On the other hand, the emergence of data-processing industries catalyzed a discussion that personal data requires protection based on choice, rather than harm; on property, rather than liability. For example, Lawrence Lessig contends that "a property regime requires negotiation before taking; a liability regime allows a taking, and payment later."[156] Under the property rules, it is an individual who would decide how much his or her personal information costs.[157] Under a liability regime, this control leaves the private hands and shifts to a court, a jury, or a statute.[158] It affords only as much compensation as a reasonable person deems necessary. In the meantime, the property regime would protect equally a person who values her data and one who does not. Each can choose how much to take in exchange for disclosure of valuable information.[159] An example of the property-based data exchange is a modern preferred-customer card. Offering the card, stores extend discounts to shoppers in exchange for their consent to having their identity and spending habits shared.

Despite the advantages of the private self-regulation approach, it has posed a considerable challenge to U.S. policymakers in recent years. In fact, although the United States has not created any special data protection authority, social concern triggered the decision to delegate certain oversight mandates to the U.S. Federal Trade Commission (FTC).[160] In accordance with the FTC's 2000 survey, ninety-two percent of individuals from online households stated that they do not trust online companies to keep their personal information confidential, and feel that self-regulatory initiatives are insufficient.[161] Thus, "only eight percent of heavily

153. MANN & WINN, *supra* note 123, at 152.

154. SOLOVE & ROTENBERG, *supra* note 11, at 492.

155. William Challis & Ann Cavoukian, *The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective*, 19 MARSHALL J. COMPUTER & INFO. L. 1, 20 (2000).

156. SOLOVE & ROTENBERG, *supra* note 11, at 510–12.

157. *Id.*

158. *Id.*

159. *Id.* at 510 (quoting LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999)).

160. *Id.* at 541.

161. U.S. FEDERAL TRADE COMM'N, FAIR INFORMATION PRACTICES IN THE ELECTRONIC

trafficked websites display a seal from one of the self-regulatory seal programs."[162] As Marc Rottenberg contends, the "privacy policy in the United States today reflects what industry is prepared to do rather than what the public wants done."[163] Eighty-two percent of the respondents to the FTC's survey suggested that government should regulate online companies' use of personal information.[164] Advocates of statutory supervision suggest that private regulation does not consider that the use of data provides "access to social power."[165] When the law starts treating personal data as an economic asset, it divides the people by "those who can afford privacy and those who cannot."[166]

C. Micro-Structure of the Western Data Protection: The Solidity of Definitions or the Flexibility of Principles?

In terms of setting an effective micro-structure for data protection, a comprehensive statute can provide a wealth of clear-cut, harmonized rules and definitions that will promote uniformity and certainty in enforcement. On the other hand, statutory definitions may turn out to be artificial, stiff, and quickly outmoded, especially in the face of rapid technological advances. Self-regulation, in turn, presents a danger of ad hoc, messy, and incoherent setting of standards. However, it provides a much better opportunity for gradual evolution of viable concepts which would correspond to the social awareness and would easily adapt to any new conditions.

The European Directives offer a well-organized treasury of terms and rules. For example, article 2 of the General Directive defines the key terms "personal data," "processing," "filing system," "controller," "processor," "third party," and "data subject consent."[167] Further, the Directive establishes six conventional principles forming the "skeleton" or the "core" of the microstructure for data protection:

MARKETPLACE PRIVACY ONLINE, A REPORT TO CONGRESS 2 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [hereinafter FTC REPORT].

162. *Id.* at 35.

163. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 119.

164. FTC REPORT, *supra* note 161, at 2.

165. Katrin S. Byford, *Privacy in Cyberpace: Constructing A Model of Privacy for the Electronic Communication Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 56 (1998).

166. *Id.* at 57.

167. General Directive, *supra* note 111, art. 2.

> (1) *legitimacy*: personal data may only be processed for limited purposes; (2) *finality*: personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes; (3) *transparency*: the data subject must be informed regarding data processing related to him; (4) *proportionality*: personal data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and processed; (5) *confidentiality and security*: technical and organizational measures to ensure confidentiality and security must accompany processing of the data; and (6) *control*: DPAs must ensure supervision of processing.[168]

In addition to offering a working scheme for data protection, the European directives present the most advanced product of harmonization in the field. They present a compelling guidance for setting legislative frameworks in all members of the EU. Furthermore, the language of the General Directive largely reflects the language of the Council of Europe Data Protection Convention and the OECD Guidelines—the documents, adopted in consultation with the vast majority of developed non-EU economies, including Japan, Canada, the United States, and Australia.

However, clear-cut definitions and stringent principles still possess the implicit danger of easily becoming outdated. The field of data protection is directly affected by technological developments.[169] One of the common criticisms of the General Directive is that it was drafted in an era of mainframe computers and may cope poorly with the advance of Internet technology.[170] For example, the general definition of personal data as "any information relating to an identified or identifiable natural person"[171] seems to stretch easily to a variety of settings. Nevertheless, it remains unclear if an email, a dynamic IP address, clickstream information, or log files are embraced by this definition.[172] Paradoxically, the benefits of clear-cut formulas for data protection may hinder, rather than advance certainty in the context of technological development.

American data protection law largely evolved in the absence of statutory language.[173] This allowed private actors to set the policies to their liking, and, in order to ensure fairness, provided the common law courts

168. KUNER, *supra* note 104, at 17–18.
169. *Id.*
170. *Id.*
171. General Directive, *supra* note 111, art. 2(a).
172. SOLOVE & ROTENBERG, *supra* note 11, at 721.
173. *See id.* at 2–25.

with vast discretion to determine which concepts are just.[174] The first developments in American information privacy law, albeit only in the form of persuasive authority, emerged in a law review article tailored to the social concern.[175] In the later nineteenth century, the rise of yellow journalism and technological inventions, such as instantaneous photography, which facilitated intrusions into private lives, inspired Samuel Warren and Louis Brandeis to publish the article, *The Right to Privacy*.[176] The authors suggested that as the need to secure the right "to be let alone" increases with the advance of civilization, the common law should "meet the new demands of society . . . without the interposition on the legislature."[177]

Following this appeal, in 1905 Georgia became the first state to recognize a common law tort action for privacy invasions.[178] In *Pavesich v. New England Life Ins. Co.,* a Georgia court penalized a newspaper for publication of the plaintiff's picture on a life insurance advertisement without his consent.[179] The court concluded that "[t]he right of privacy has its foundation in the instincts of nature. It is recognized intuitively, consciousness being the witness that can be called to establish its existence."[180]

It would be unfair to say that all courts in the United States endorse non-statutory legalization of the data protection framework. Public debate continues as to how much discretion judges, as opposed to legislatures, should hold.[181] In fact, the first case citing *Right to Privacy, Roberson v. Rochester Folding Box Co.*, declined to implement protection of privacy absent a statutory framework.[182] The *Roberson* court found it permissible to publish a lithograph on the advertisements without authorization of the model, because there was neither statute, nor precedent banning such publication. The court held that "[t]he courts . . . being without authority to

174. *See id.*

175. *See* Warren & Brandeis, *supra* note 117. *See also* SOLOVE & ROTENBERG, *supra* note 11, at 3–5.

176. *Id.* at 3.

177. Warren & Brandeis, *supra* note 117, at 195. *See also* SOLOVE & ROTENBERG, *supra* note 11, at 193–95.

178. SOLOVE & ROTENBERG, *supra* note 11, at 65 (citing Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905)).

179. 50 S.E. 68, 68–69 (Ga. 1905).

180. *Id.* at 69.

181. Examples of "pro-statutory" cases include J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) and Am. Fed'n of Gov't Employees, AFL-CIO v. Dept. of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997) (expressing the court's "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information.").

182. 64 N.E. 442 (N.Y. 1902).

legislate, are required to decide cases upon principle. . . ."[183] Afraid to bring incoherence to the legal system by an arbitrary judgment of the first impression, the court further concluded, "the mischief which will finally result [from an arbitrary application of a principle] may be almost incalculable under our system, which makes a decision in one case a precedent for decisions in all future cases."[184]

Even Warren and Brandeis recognized that court-devised limitations as to concrete factual situations made the doctrine difficult to apply, and "to a certain extent uncertain in its operation and easily rendered abortive."[185] Studying a line of privacy cases, an outsider can get easily confused, as the approach differs from circuit to circuit. For example, *Cline v. Rogers*[186] establishes that an individual has no constitutional right to privacy in her criminal record. *Paul v. Verniero*[187] upheld a law authorizing police to notify the community if a new neighbor was a sexual offense convict. However, *Briscoe v. Reader's Digest Ass'n*[188] and *Melvin v. Reid*[189] punished the media for revealing the names of a former prostitute and a former hijacker, despite that the names came from the public court record. To reconcile seemingly conflicting precedents under the self-regulatory U.S. court system, one needs to match facts to a policy, not a rule.[190] In the absence of definitions, courts develop principles of social policy to scrutinize disputed conduct. For instance, in his famous concurrence in *Katz v. United States,* Justice Harlan suggested a two-fold test to assess whether privacy was violated: "first . . . a person [must] have exhibited an actual (subjective) expectation of privacy and, second . . . the expectation [must] be one that society is prepared to recognize as 'reasonable.'"[191]

Flexible non-statutory definitions, although messy, offer an important advantage that the statute cannot provide. They allow the court to adapt any rule or concept to society's concept of fairness at a certain time in its evolution. As Kathryn Hendley observed, "[p]erhaps the concept of

183. *Id.* at 443.
184. *Id.* at 444.
185. Warren & Brandeis, *supra* note 117, at 215–16.
186. 87 F.3d 176, 179 (6th Cir. 1996).
187. 170 F.3d 396, 405 (3d Cir. 1999).
188. 483 P.2d 34, 43–44 (Cal. 1971).
189. 297 P. 91, 93–94 (Cal. 1931).
190. Not only can an outsider become confused by the contradictions within U.S. privacy case law, but the conflicting standards are also troublesome to a civil law attorney with great familiarity with the U.S. legal system. While the privacy cases may originate from a variety of jurisdictions, all of the cases purport to interpret the Constitution. Even between this Article's two authors, these contradictions were less troublesome to the common law attorney than to the civil law attorney.
191. 389 U.S. 347, 361 (1967).

'private property,' ostensibly the ultimate material incentive, should be applied to both the state and the law per se—it is 'our' state, and the law belongs to us, too."[192] When definitions are easily adaptable to technological evolution and contextual circumstances, it is the social demand that shapes the supply of legal rules, not vice versa; the citizens are urged to put trust into their state and law.

D. Data Protection Versus Free Flow of Information: The Art of Balancing

The micro-structure of definitions versus principles tangibly affects the balancing of data protection with free information flow. The European General Directive defines balancing proactively, by establishing sets of *a priori* defaults and exceptions. The U.S. courts are doomed to engage in balancing reactively as they weigh the arguments of two conflicting parties. As a consequence, statutory balancing is more likely to shift the defaults from freedom of information to protection of data. Because under self-regulation the law is silent unless a data subject actively stands up, the default allows a data controller to use the information as he pleases. When a legislature decides to adopt a data protection statute, the name and purpose of the statute itself suggest a default in favor of data protection. Free flow of information might obtain regard through exceptions if the legislature opts to put them in place. As a consequence, adoption of a data protection statute likely will shift the balance away from the free flow of information, even if the statute were liberally phrased.

1. A Restrictive Default in the World of Statutes

Article 1 of the General Directive expressly defines the object of its regulation as: (1) to protect [the right of natural persons] to privacy with respect to the processing of personal data and (2) to ensure free flow of personal data between the member states.[193]

The European default restricts any operations with personal data unless a specific exception applies.[194] For example, article 8 bans processing of sensitive data in paragraph (1) but paragraphs (2)–(5) enumerate as many as nine exceptions making such processing legitimate.[195] Similarly,

192. Kathryn Hendley, *Demand for Law: Rewriting the Rules of the Game in Russia: The Neglected Issue of the Demand for Law*, 8 E. EUR. CONST. REV. 89, 95 (1999).

193. General Directive, *supra* note 111, art. 1.

194. *Id.* art. 7.

195. *Id.* art. 8, ¶¶ 1–5.

paragraph (1) of article 11 imposes a demanding notification requirement on data controllers, while paragraph (2) specifies conditions for release from the obligation.[196] Additionally, paragraph (1) of article 18 requires that data controllers notify supervisory authority before carrying out automatic processing of personal data, but paragraph (2) of that same section provides the circumstances when this notification requirement may be simplified or exempt.[197] Exceptions favoring the free flow of information are purpose-based. The General Directive enumerates exceptions for statistical, scientific, historical research processing,[198] journalism,[199] the benefit of the data subject,[200] and others. The exceptions are deliberate, concrete, and generally immediately follow the restrictions they cancel. Such a structure both facilitates the information balancing process, and reiterates the concurrence of interests in free flow of information and in protection of data.

In spite of the statute's attempt to provide careful balancing, the European Commission has received criticism that the current regime is overly restrictive on private controllers.[201] The complaints suggest that "certain provisions of the General Directive, impose onerous requirements that are out of proportion to their value in protecting the privacy rights of data subjects (the legal regime for notification of data processing is an example)."[202] For example, in the recent *Lindquist* case (Sweden), the local data protection authority (DPA) imposed a fine on a church volunteer. The volunteer, who tried to enhance interaction between the church members, created a website with their names, contact information, and hobbies, without first obtaining their consent or consulting the DPA in advance. The DPA was especially concerned about posting information that one church member had recently injured her foot, as health data falls under a special category of protection as "sensitive."[203] On another occasion, the Spanish DPA imposed a fine of 10 million pesetas (approx. 60,000 Euro) on Microsoft Iberica SRL for processing personal data without the consent of data subjects.[204] Calling for amendments, the Swedish Ministry of Justice, for example, concluded that "[i]n order for

196. *Id.* art. 11, ¶¶ 1–2.
197. *Id.* art. 18, ¶¶ 1–2.
198. *Id.* art. 6.
199. *Id.* art. 9.
200. *Id.* art. 7(d).
201. Commission Report, *supra* note 103.
202. KUNER, *supra* note 104, at 47.
203. Case C-101/01, Lindquist v. Aklagarkammaren I Jonkoping.
204. KUNER, *supra* note 104, at 38.

the provisions to gain acceptance and to have a real breakthrough in their practical application, they must be simplified and concentrate on the essentials, namely, for protecting against harmful acts in the nature of misuse."[205]

In response to the complaints, however, the Commission rebuts that the problem is not the statute, but the enforcement. Per the Commission, the enforcers do not take advantage of the exceptions from the default restrictions as much as they should.[206]

2. A Laissez-Faire Default in the No-Statute World

In the United States, by contrast, the absence of a restrictive statute has given data controllers a default of free conduct with data unless a data subject acts affirmatively to impose a restriction. Moreover, this default is reinforced by the constitutional right to freedom of speech. In First Amendment free speech cases, commercial controllers are subject to "intermediate scrutiny," while the media, because of its "democracy watchdog" status, enjoys an almost absolute protection.[207]

The concept of intermediate scrutiny established by *Central Hudson Gas & Electric Corp. v. Public Service Commission of N.Y.*[208] enables the government to impose restrictions on lawful, non-misleading commercial speech only if: (1) the government has a substantial interest in regulating the speech; (2) regulation directly and materially advances that interest; and (3) regulation is no more extensive than necessary to serve the interest.[209] The effect of intermediate scrutiny analysis is that the government avoids direct restriction wherever possible; however, it does uphold an individual's restrictive action. For example, in *U.S. West Inc. v. FCC*, the court invalidated a Federal Communication Commission (FCC) order requiring telecommunications companies to seek consumer approval before using a customer's personal information for marketing purposes.[210] The court reasoned that the FCC:

> merely speculate[s] that there are a substantial number of individuals who feel strongly about their privacy, yet would not

205. *Id.* at 48 n.198 (quoting Swedish Ministry of Justice, Simplified protection for personal data applying misuse model (Nov. 30, 2000) (unpublished memorandum)).

206. Commission Report, *supra* note 103, at 24.

207. Hudson Gas & Electric Corp. v. Public Service Commission of N.Y., 447 U.S. 557 (1980).

208. *Id.*

209. *Id.* at 564.

210. 182 F.3d 1224, 1228 (10th Cir. 1999).

> bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.[211]

Media enjoys almost absolute protection. Social policy tries to shield the media from the threat of lawsuits, to make sure that "media is not 'chilled' from running certain stories if the state starts imposing on it costs for gathering, producing, and disseminating news."[212] In *Bartnicki v. Vopper*, the court struck down the Wiretap Act's provision expressly prohibiting publication of unlawfully intercepted conversations, when the information published was of public interest.[213] The plaintiff, a labor union leader, suggested on the phone to his colleague that they should resort to violence if the union's demands were not met.[214] When the defendants found a tape of the conversation intercepted by a third party and broadcast it on the radio, they were released from liability for such use of personal information.[215]

However, as Daniel Solove argues, the law recognizes the "great potential for media information gathering to become intrusive and harassing, especially when a person becomes the subject of a prominent story."[216] Under such circumstances, the law does restrict the media's conduct in its collection of information and its choice as to what to publish. For example, in *Gallela v. Onassis*, the Second Circuit Court of Appeals ruled against a paparazzo who had committed a series of obnoxious actions interfering with life of the famous Onassis family.[217] In *Gallela*, the court held that "[c]rimes and torts committed in news gathering are not protected by the First Amendment. . . . There's no threat to free press in requiring its agents to act within the law."[218] The Ninth Circuit, in *Dietemann v. Time* penalized a newspaper for the secret use of a hidden camera and tape recorder in the home of a poor, uneducated medicine man, to collect evidence to ridicule his medical beliefs.[219] However, in *Desnick v. American Broadcasting Co., Inc.*, the Seventh Circuit refused to penalize the media for an "undercover investigation" aimed to reveal fraud and abuse in a well-established and recognized

211. *Id.* at 1239.
212. SOLOVE & ROTENBERG, *supra* note 11, at 117.
213. 200 F.3d 109, 130 (3d. Cir. 1999), *aff'd*, 552 U.S. 514 (2001).
214. *Id.* at 113.
215. *Id.*
216. SOLOVE & ROTENBERG, *supra* note 11, at 69.
217. 487 F.2d 986 (2d Cir. 1973).
218. *Id.* at 995–96.
219. 449 F.2d 245 (9th Cir. 1971).

clinic.[220] The court reasoned that unlike in *Dietemann*, this investigation was not conducted within the subject's home; the social interest to prevent fraud in a licensed clinic was substantial; and the undercover investigation, although deceptive, did not disrupt operation of the institution.[221]

Non-statutory flexibility allows a delicate balance in each controversy presented before the court. However, such a scheme relies heavily on the adequacy of various legal institutions. In the absence of statutory guidance and enforcement, private controllers have an incentive to restrict use of personal data only when they fear lawsuits. This fear materializes only if individuals are willing to go to court. This willingness, in turn, is predicated on the professionalism and morality of judges. Finally, the high morality of judges is not nourished without the free flow of information to allow for easy criticism of incompetent judges and biased decisions. The social value of free information flow in such a system closes the circle by establishing a default against personal data privacy.

In recent years, the United States has found its privacy system inefficient. As fear of lawsuits can motivate self-censorship of private data controllers, data subjects fear that their personal information will be abused in the absence of a stricter regulation has motivated self-censorship of their engagement with private businesses. In its 2002 study, the research facility, Media Jupiter Metrix, estimated that privacy and security concerns could cost online vendors almost 25 billion by 2006.[222] As Avivah Litan, a leading analyst from the Gartner Center, once exclaimed: "People are paranoid; they don't want to give their information away and they have a right to be paranoid."[223]

Social concern prompted Congress to restrict the default rule of free commercial speech through legislation regarding sensitive data. For example, the Video Privacy Protection Act (VPPA),[224] prohibits videotape service providers from knowingly disclosing personal information, such as titles of video cassettes rented or purchased, without the subject's written consent. The Telephone Consumer Protection Act (TCPA) prohibits use of a fax machine to send unsolicited messages.[225] The Fair Credit Reporting Act (FCRA) requires credit reporting companies to provide individual

220. 44 F.3d 1345 (7th Cir. 1995).

221. *Id*. at 1351–54.

222. Robert Leathern, Jupiter Media Metrix, Online Privacy, Vision Report (2002), *at* http://www.jup.com/bin/item.pl/search/ (guest registration required).

223. Joe Wilcox, Study: Customers Wary of Online Ads, *at* http://news.com.com/2100-1001-892808.html.

224. 18 U.S.C. § 2710 et. seq. (2002).

225. 47 U.S.C. § 227 (1991).

access to records, establishes procedures for correcting erroneous personal information, and sets limitations on disclosure.[226]

The EU statutory mechanism and the U.S. non-statutory mechanism each present important benefits to their constituencies while challenging them with their shortcomings. The statute allows Europeans to regulate data privacy as an important social value, to create a clear-cut system of rules and definitions, and to balance freedom of speech and privacy through an established set of imperative defaults in favor of data protection with important exceptions for information flow in return. However, one must ask whether society needs the government to spend resources on proactive public enforcement if definitions become easily outdated, and if balancing imposes an undue burden on development of the private sector. Self-regulation has allowed the United States to give individuals and companies extensive choice as to data processing practices; to facilitate development of adaptable, up-to-date rules and definitions; and to advance the free flow of information as a safeguard to a democratic society. At the same time, it created threats of inadequate protection for an important value, haphazard precedent setting, and reluctance of the individuals to engage with data-collecting industries for the fear of data misuse.

Which approach's advantages would be more tangible, if applied to the Ukrainian context? What drawbacks of each, when planted into the Ukrainian soil, will show up faster? Let us now turn to transplantation in context, as we return to a fork in the decision-making road for Ukraine.

IV. TO HAVE OR NOT TO HAVE: WHAT IS THE SOLUTION?

As both approaches have their drawbacks, Ukraine cannot choose between black and white. Borrowing the foreign experience, it must rather resort to comparing shades of gray. One ultimate issue in the balancing test is to determine the default and weigh the costs of transition against the benefits of optimization. As Frederick Schauer suggested, "[c]haracteristic modalities of law are ones that are premised, at least in part, on stability for stability's sake, and thus on the view that in some or many contexts the costs of transition to a new rule exceed the benefits of optimization."[227] Because the current default in Ukraine is set at no omnibus data protection

226. 15 U.S.C. § 1681 et. seq. (2002).

227. Frederick Schauer, *Legal Transitions: Is There an Ideal Way to Deal with the Non-Ideal World of Legal Change?: Legal Development and the Problem of Systemic Transition*, 13 J. CONTEMP. LEGAL ISSUES 261, 265 (2003).

statute, the issue boils down to balancing costs and benefits of changing this default rule and transitioning to a scheme regulated by an omnibus statute.

What benefits will Ukraine gain if the default rule is changed, and what are the costs and risks of obtaining these benefits? Is the country ready to pay these costs and internalize the losses? How great is the cost of non-transition if the country cannot embrace transition successfully?

A. Costs of Transition for Macrostructure: Lack of Enforcement Resources

1. Benefits of Transition to the Statute for the Macrostructure of Data Protection

To build a social-law-based state where the goal is not a laissez-faire economy, but rather "human rights and freedoms,"[228] an omnibus statute does advance a macrostructure of the law on data protection. Lack of a comprehensive statute to provide for public enforcement may cause Ukraine to overlook its constitutional obligations, as well as its obligations under the European Convention of Human Rights. This concern can be demonstrated by the fact that in the United States, where the Constitution implicitly safeguards privacy, it recently has been recognized that self-regulation alone provides insufficient protection to the social value of information privacy.

The U.S. Federal Trade Commission was an active proponent of business self-regulation at the start of its involvement with the privacy issues.[229] However, in 2000, after the Commission conducted comprehensive monitoring of such self-regulation results, it was forced to concede its strategy's failure and to call for the adoption of major new legislation.[230] By contrast, the European authorities acknowledge that there is much room for criticism of the General Directive, but find current data protection shortcomings incidental to, rather than inherent in, legislative regulation.[231] In its 2003 Report, the European Commission concluded that the "[General] Directive fulfilled its principal objective of removing barriers to the free movement of personal data between the member states"[232] and decided that no amendments were needed.[233] As Internal

228. UKR. CONST. art. 3.
229. MANN & WINN, *supra* note 123, at 169.
230. *Id.*
231. *Commission Report*, *supra* note 103, at 7.
232. *Id.* at 10.

Market Commissioner Frits Bolkestein summarized, "European citizens have a right to privacy . . . . [The] Directive has helped make sure that they can enjoy that right in practice."[234]

In addition to the European developments, the recent call for a privacy statute in the United States reinforces the position that implementation of a privacy statute is right for Ukraine if it is to fulfill its obligations under the Constitution and the European Convention.

2. Costs of Transition to the Statute for the Macrostructure of Data Protection

While a number of facts support the general idea of introducing a data protection statute in Ukraine, its implementation in the short term may bring an adverse result. The cost of transition will require allocation of sufficient resources for fair public enforcement. Modern scholarship warns that legal standards that work well in developed countries sometimes prove to be too ambitious when transplanted into a less efficient system.[235] Even the strong European economy finds it challenging to provide resources for enforcement of the data protection law. In its 2003 *Report on Transposition of the General Directive*, the European Commission recognized that enforcement had been "under-resourced," compliance by data controllers was "very patchy," and data subjects had an "apparently low level of knowledge of their rights."[236] A "Eurobarometer" survey showed that only forty-six percent of EU companies inform data subjects of the purposes of the processing.[237] In accordance with another study, as many as ninety percent of German internet merchants do not comply fully with data protection laws.[238]

If Germany, with a gross national product (GNP) of 22,740 USD per capita for 2004,[239] cannot provide resources for better compliance, what

233. *Id.* at 7–8.

234. Press Release, European Commission, Data protection: Commission Report Shows that EU Law is Achieving Its Main Aims (May 16, 2003), *available at* http://europa.eu.int/rapid/PressRelease.do?reference=IP/03/697&format=PDF (last visited Jan. 6, 2006).

235. FLORENCIO LOPEZ-DE-SILANES, THE POLITICS OF LEGAL REFORM YALE UNIVERSITY AND NBER G-24 DISCUSSION PAPER NO. 17 (2002).

236. *Commission Report*, *supra* note 103, at 12.

237. *Eurobarometer*, *supra* note 139.

238. KUNER, *supra* note 104, at 118 (quoting Marie-Anne Winter, *Online Shops: 90 Prozent am Rande der Legalitat,* Jan. 16, 2001, *available at* http://www.teltarif.de/intern/action/print/arch/2001/kw03/s4076.html (last visited Jan. 6, 2006)).

239. WORLD BANK, WORLD DEVELOPMENT INDICATORS DATABASE 1 (2004), *available at* http://www.worldbank.Org/data/countrydata/htm (last visited Jan. 6, 2006).

can be expected of Ukraine, with its 780 USD per capita GNP?[240] Concern about lack of enforcement resources has become an essential argument against adoption of the current Bill on Data Protection in debates and discussions. As participants of the parliamentary roundtable in February 2003 perceived, there is a "concern regarding the existence in Ukraine of a gap between fair requirements of the adopted laws and the practice of implementation."[241] The economic situation makes it unlikely that Ukraine will create a Data Protection Authority of a least comparable efficiency to its European counterparts.

While resources are always scarce, in a healthy and stable state, the importance of omnibus enforcement is not necessarily a central issue. Selective and sudden state action can work just as well, offering a vaccine against violations by setting examples through successful prosecutions. However, in the context of Ukraine's transition to democracy, patchy and selective public enforcement may cause more harm than no public enforcement at all. Ukraine is not yet healthy and stable, still weakened by the difficulties of economic and political transition. These difficulties have catalyzed the epidemic of corruption and inspired a certain nostalgia for authoritarian order. In accordance with Transparency International's Corruption Perception Index, Ukraine is ranked nineteenth most corrupt among almost 150 countries ranked.[242] By way of comparison, the United States ranks 128th while the EU countries rank between seventy-first for Poland and 146th for Finland.[243] In 2003, the International Foundation for Election Systems (IFES) Survey for Ukraine indicated that only twenty-nine percent of Ukrainians trusted the Cabinet of Ministers, twenty-six percent trusted the Parliament, and twenty-two percent trusted the President to act in good faith.[244]

Recently the Orange Revolution, a large civic uprising at the end of 2004, brought the attention of the entire international community to the massive falsification of the voting results in the Ukraine's presidential elections. Under

240. *Id.* at 2.

241. Global Internet Policy Initiative (GIPI), *Zasidann'a Sektsiji Pryvatnist'/Publichnist' informatsiji* [*Meeting of the Section Privacy/Publicity of Information*], *available at* http://gipi.internews.ua/ukr/activity/initiatives/seminars/0228_deference.html (last visited Jan. 6, 2006) [hereinafter GIPI].

242. TRANSPARENCY INTERNATIONAL, CORRUPTION PERCEPTION INDEX 2004, 5 (2004), *available at* http://www.transparency.org/pressreleases_archive/2003/2003.10.07.cpi.en.html (last visited Jan. 6, 2006).

243. *Id.*

244. RAKESH SHARMA & NATHAN VANDUSEN, IFES, ATTITUDES AND EXPECTATIONS: PUBLIC OPINION IN UKRAINE 2003, 23 (2003), *at* http://www.ifes.org/searchable/ifes_site/PDF/new_initiative/Ukraine_Survey_2003_English.pdf.

international and domestic pressure, a re-vote was held, which resulted in the installation of an allegedly pro-western candidate, Viktor Yushchenko, as Ukraine's new President. President Yushchenko announced a fight against corruption as an ultimate goal of his presidency. However, in spite of healthy optimism about renaissance of democracy in Ukraine, much skepticism remains. As an April 2005 IFES survey indicated that a plurality still contented that Ukraine is not a democracy. Sixteen percent volunteer that Ukraine is somewhere in between—they are not willing to declare Ukraine a democracy but will not concede that Ukraine is not a democracy.[245] The dismissal of the cabinet and certain other leading officials, appointed by President Yushchenko from among his closet associates within only nine months of their appointment, signified a collapse of his team under mutual accusations of corruption.

While the epidemic of corruption sweeps society, selective enforcement contributes to the weakening of the legal system's immunity against unfair practices. Creation of an additional underfunded state agency can easily create a new outlet for corruption, providing private controllers with an incentive to smooth the enforcement rather than internalize the burden of compliance.

After messy and abundant reforms in the nineties, Ukrainian society in the new century is showing considerable nostalgia for certainty and order. The IFES Survey of 2003 indicated that most people would have preferred "a strong leader who could bring order over the kind of democracy [then] practiced in Ukraine."[246] In reference to democratic reform in the former Soviet bloc countries, Acting Coordinator of U.S. Assistance Thomas Adams said, "noticeable backsliding has occurred in recent years."[247] The Freedom House 2002 Report commended former President Kuchma for his ability to hold the opposition.[248]

Although the Orange Revolution signifies a substantial breakthrough in the Ukrainian political climate, sudden change is unlikely. Recent re-privatization scandals and discord between members of the new

245. KAREN BUERKLE, LISA KAMMERUD & RAKESH SHARMA, IFES, PUBLIC OPINION IN UKRAINE AFTER THE ORANGE REVOLUTION 25 (2005), *at* http://www.ifes.org.

246. MARK DIETRICH & RICHARD BLUE MANAGEMENT SYSTEMS INTERNATIONAL, DEVELOPING THE RULE OF LAW IN UKRAINE: ACHIEVEMENTS, IMPACTS, AND CHALLENGES 3, *at* http://pdf.dec.org/pdf_docs/PNACR752.pdf (citations omitted).

247. *U.S. Assistance Programs in Europe: An Assessment: Hearing Before the Subcomm. on Europe of the H. Comm. on Int'l Relations*, 108th Cong. (2003) (statement of Thomas Adams, Acting Coordinator, U.S. Assistance in Europe and Eurasia, Bureau of European and Eurasion Affairs, Dep't of State), *available at* http://wwwc.house.gov/international_relations/108/86082.PDF (last visited Jan. 24, 2006).

248. FREEDOM HOUSE, NATIONS IN TRANSIT, UKRAINE: COUNTRY REPORT 607, *available at* http://www.freedomhouse.org (last visited Jan. 6, 2006) [hereinafter FREEDOM HOUSE].

government have resulted in paralysis of its working agenda. These problems show the system's susceptibility to massive usurpation of enforcement powers by a certain political force to advance private, rather than public goals.[249] Agencies may raise a "selective sword" when the governmental interest in data protection or the interest to suppress someone's business is greater than the agency's under-resourced enforcement capacities.

There is a recent trend of using "selective sword" enforcement as an effective tool for taming the opposition, in conjunction with other seemingly democratic statutes. For example, during the recent presidency of Leonid Kuchma, Judge Zamkovenko, Chief Judge of a trial court in the capital city of Kyiv, had received a number of awards and commendations for his dedicated service until 2001. After several decisions unpopular with the government, the Supreme Council of Justice opened an investigation on corruption charges against the judge himself.[250] The investigation uncovered that the judge had a legacy of intentionally withholding case files to delay citizens' court appeals.[251] Although litigants had lodged complaints about the judge for years, an investigation was not started until decisions passed that were unpopular with the government.[252]

In view of insufficient enforcement resources in the foreground of corruption and the significant authoritarian legacy, transition to a data protection statute to enhance public value of information privacy may be prohibitively expensive for the short term. Unable to cope with the costs, the legal system may be tempted to privatize enforcement further in the hands of the minority of the most dishonest players, instead of advancing the country's aim to comply with the international human right standards and its own constitutional obligations.

---

249. *See, e.g.*, *Yushchenko's Popularity Sliding*, CNN, Sept. 8, 2005, *at* http://www.cnn.com (last visited Oct. 2, 2005); *Ukraine Tycoon Hopes Firing Government Will End Re-privatization*, FORUM, Sept. 14, 2005, http://en.for-ua.com/news/2005/09/14/155016.html (last visited Jan. 6, 2006).

250. *Id.*

251. U.S. DEP'T OF ST., BUREAU OF DEMOCRACY, HUMAN RIGHTS, AND LABOR, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES FOR 2002: UKRAINE (Mar. 31, 2003), *available at* http://www.State.gov/g/drl/rls/hrrpt/2002/18398.htm (last visited Jan. 6, 2006).

252. The Ukrainian newspaper, *Zerkalo Nedeli*, presents a number of arguments regarding Judge Zamkovenko's illegal actions, which went unpunished until he adopted a wrong decision in the politically sensitive Timoshenko case. Alexandra Primachenko, *The Inside of the Judge's Robe,* 46 (471) ZERKALO NEDELI (Nov. 29, 2003–Dec. 5, 2003).

B. Impact of Cost of Transition on Microsctructure: Lack of Demand

1. Benefits of Transition to the Statute for the Microstructure of Data Protection

Analysis of transitional implications on microstructure of the data protection framework yields similar results. Adoption of a statute promises important advantages over self-regulation, but the cost of obtaining them makes it reasonable to postpone the transition.

Although the European Directives are sometimes criticized as outmoded and stiff, changing an outmoded statute takes less time than stirring an evolution of policy-based judicial precedents from Ukraine's civil law tradition. In the absence of a backbone statute, the Ukrainian justice system may be unable to turn the chaos of scattered norms and provisions into an orderly, structured legal policy. Even U.S. privacy case law shows a lack of unanimity among judges. In Ukraine, where legal textbooks even recently matched the term "judicial law-making" with the term "arbitrary," and where the Supreme Court Chief Justice complains that "[f]or centuries the judicial power has been portrayed as insignificant, constantly hindering somebody and doing everything wrong,"[253] judges may be not eager to take on leadership in defining the scope of actual data protection.

The Ukrainian judiciary does not have a history of independent judgment. The cost of not transitioning to a statute is a growing loss of hope that the justice system will sculpt the microstructure of information privacy through policy-based interpretation, as the U.S. justice system did. However, the transition will require that the legislature, instead of the judiciary, shape needed rules and definitions. The question arises whether the legislature or judiciary is better equipped to articulate the appropriate microstructure.

2. Costs of Transition to the Statute for the Microstructure of Data Protection

Unlike the judiciary, which can have years to tailor policies in response to emergent social concerns, the legislature must do so expediently. It is important to remember that in the European Union and western Europe, state legal action against misuse of personal data by private controllers

253. BBC Monitoring Online, *Ukrainian Chief Judge Interviewed on Judicial System* (Mar. 28, 2003), http://www.monitor.bbc.co.uk/database.shtml (subscription required).

took place only after social concern emerged, long after the free flow of information was a rooted democratic value. In Ukraine this is not the case. The goals of freedom of information and protection of privacy only recently have been imported into the mainstream official culture. Analyzing failures of the Russian business law reforms, Kathryn Hendley suggested lack of demand for law as an important reason: the catchphrase "if you build it, they will come," does not seem to work in transplanting a reform.[254] "Before any type of legal reform can take hold in the Ukrainian society, Ukrainians themselves have to genuinely believe in and take ownership of reform ideas, principles, and theories."[255]

The demand for a statute regulating private data controllers has not ripened yet in Ukraine's society. The public has not begun to perceive a threat to personal inviolability by private data control. Most individuals in Ukraine receive salaries and transact in cash, and few have bank accounts. Medical records are held largely in governmental clinics and rarely are computerized. The direct advertisement business is taking its first steps. Valentyn Kalashnyk, director of the five-year-old direct marketing company OS Direct, shared in an interview with a business journal that, although the Constitution and the Law on Information provide a cause of action for privacy intrusions, his company had not had any lawsuits.[256] In the six months preceding the interview, at most five customers had objected to OS Direct's use of their personal data.[257] Although computer technology has been penetrating at an increasing rate, it has not reached nearly a critical mass of the population to give rise to the prosperous data-collection businesses. For example, although the number of Internet users in Ukraine is reported to have grown from only 400 people in 1993 to 900,000 people in 2002,[258] in relation to the total population of nearly 50 million, this number constitutes less then one percent. Further, among these users, only twenty-two percent in 2001 and six percent in 2002 made online purchases.[259] According to the UNDP Report, consumer doubt as to

254. Hendley, *supra* note 192, at 89.

255. Kim Ratushny, *Toward the "Independence . . . of Judges" in Ukraine?*, 62 SASK. L. REV. 567, 584 (1999).

256. *Id.*

257. A. Kashpur, *Dyrekt-Marketing Staje Nebezpechnym* [*Direct Marketing Becomes Dangerous*], 34 HALYTSKI KONTRAKTY (2000).

258. United Nations, Dep't of Economic and Social Affairs, Statistics Division, Millennium Indicators: Ukrainian Country Profile, http://unstats.un.org/unsd/mi/mi.asp (Choose "Ukraine" under Step 1; Choose "1990–2005" under Step 2) (last visited Jan. 6, 2006).

259. UNDP REPORT, *supra* note 19, at 31.

the quality of goods, and the limited use of credit cards as a payment system will keep the trend stable for some time.[260]

One may argue that the apparent lack of data collection by businesses does not justify postponing a data protection statute. Currently, as technology is developing rapidly and the country wants to ensure human rights and growth of international cooperation, adopting a statute in anticipation of business would allow businesses and judges to react gradually.

Instead of channeling future relations in the right direction from their inception, a data protection statute in advance of its demand articulates a clear need for particular provisions, and unfortunately, aggravates the risk of imposing artificial and incoherent restrictions. This risk exists even if borrowing European concepts rather than inventing Ukraine's own costly remedy. Already, the European terms often are labeled as outmoded. Moreover, the Ukrainian context might be different and the law could create even more ambiguities and uncertainties than its absence. Analysis of the language of the Bill on Data Protection demonstrates that current lawmakers are not much more in the loop than is the current system of justice. For example, the Bill establishes that personal data is property of the data subject. It further states, "the right to property in personal data is absolute, inalienable, inviolable, and inseparable."[261] The Constitution defines property rights as the owner's authority to possess, use, and dispose of an object at the owner's full discretion.[262] It is unclear how the concept of inalienable property will fit into this definition. While the authors maintain that this approach is more advanced than that practiced abroad,[263] it suggests a hybrid of the European inalienable human right and the U.S. valuable tradable commodity. Before data collection business takes its roots, the choice of the right formulations may become an overly burdensome task for lawmakers.

Unless a statute first evolves in social awareness and then becomes transposed onto paper, it will not resolve the civil law judiciary's desire for certainty. As European experience indicates, technology renders terms obsolete with amazing speed. Once this happens, the judiciary's challenge to comply with an antiquated statute will be even greater than the challenge to create fair rules of interpretation of the general constitutional principles in the absence of a detailed statutory instruction.

---

260. *Id.*
261. Bill on Data Protection, *supra* note 92, art. 7.
262. UKR. CONST. art. 41.
263. BARANOV, *supra* note 65, at 126.

3. Costs of Non-Transition to the Statute for the Microstructure of Data Protection

In the absence of a statute, primary rulemaking authority will not fall upon judges, but rather on private businesses, organizations, and individuals themselves. Although the U.S. Federal Trade Commission found self-regulation insufficient, it acknowledged that the industries had achieved significant success in setting initial standards.[264]

Through trial and error and competition, private controllers in Ukraine will be better positioned and more motivated to harmonize the active framework using the best foreign practices, than the legislature, which is pressured by foreign donors and lacking in empirical experience. As time passes, private self-regulation may prove insufficient for protecting the rights of individuals. Even in the longstanding laissez-faire U.S. economy, the need to mend self-regulation with sectoral statutes has been acknowledged. However, once a society develops new sets of relations and sees a concrete threat of harm to the personal data associated with these relations, the cost of transitioning to a new statute will shrink compared to the cost of non-transition. Social institutions and legislature will be better suited to demand and supply, respectively, an adequate statute.

Until then, it is unfair to claim nascent businesses have no guidance in setting data-processing practices, and data subjects have no redress to violations of their privacy rights. The current framework is messy, but if handled professionally, it can provide a European-style protection to individuals. For example, the Law on Information establishes principles of collection and storage minimization, notification, consent, and access with regard to processing personal information.[265]

Furthermore, the current Ukrainian Constitution has a direct impact,[266] by allowing individuals to assert their constitutional rights regardless of whether interpretive legislation exists.[267] The direct effect of the Constitution has been enhanced by the 2004 Civil Code's open-ended list of personality rights, whose violation may mandate damages.[268] An individual concerned with data protection can already use these instruments to demand that private controllers follow European-style use

264. FTC REPORT, *supra* note 161, at 35.
265. Law on Information, *supra* note 30, art. 31.
266. UKR. CONST. art. 8.
267. UKR. CONST. art. 55.
268. Ukr. Civ. Code arts. 440–441.

and care of data. If the private controller does not comply, the individual may demand its compliance in court.

C. Cost of Transition for Balancing

1. Benefits of Transition for Balancing the Interest in Data Protection Against the Interest in Free Flow of Information

Finally, in terms of balancing, adopting a European-style statute incorporating aspects of U.S. data protection seems most suitable for helping Ukraine integrate into the EEC and EU. The statute will allow establishment of European-style defaults in favor of data protection, and exceptions in favor of freedom of information. Consequently, flow of data between Ukraine and the EU will simplify and encourage development of business cooperation.

This harmonization of international approaches is beneficial not only for Ukraine's prospects of internet business with more remote countries, such as Germany, Italy, or France, but also the smaller scale transactions with Ukraine's traditional partners in trade and travel—Poland, Hungary, Slovakia, and other immediate neighbors that have recently joined the EU. The General Directive specifically proscribes that "transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection."[269] Because the EU is not only Ukraine's close neighbor, but also one of the largest markets for goods and services worldwide,[270] restrictions on business with the EU may disadvantage considerably Ukraine's developing economy.

2. Costs of Transition for the Balancing of Interests in Data Protection Against the Interests in the Free Flow of Information

The cost of initiating European-style balancing requires that defaults and exceptions, even if textually similar to the European statute, be interpreted and applied in the same way by the institutions. Ukraine's institutions come from a very different cultural and historical legacy then do the EU institutions. Comparing European and American balancing shows that the adoption of an omnibus data protection statute tends to shift defaults away from freedom of information. The European policy has been

269. General Directive, *supra* note 111, art. 25.
270. KUNER, *supra* note 104, at 1.

criticized for providing too much data protection, although for several generations the European culture was bred to recognize freedom of speech as a fundamental human right. By contrast, Ukraine comes from a culture without a similar history regarding freedom of speech.

Liberal Ukrainian commentators contend that transplanting a legal idea from one society to a society with a less developed moral background not only may fail to work, but may have an adverse effect.[271] It may be easier to change the written rules than the attitudes of those who interpret and apply them.[272] Such attitudes shape institutions, as they are "humanly-devised constraints that structure human interaction,"[273] without which the legal systems cannot function on the basis of legal rules alone.[274]

Can Ukraine internalize the cost of transition to new legal rules and also to institutional attitudes toward their application? Recent experience indicates that the institutional legacy can use new legal developments to advance old practices.

An introduction of the "moral harm" doctrine to the civil law presents a good illustration of this allegation. Ukraine's 1992 Law on Information allowed individuals to seek redress for interference with their right to access or disclose information by filing for damages in a civil suit.[275] Until 1993, the Civil Code's definition of damages incorporated only actual damages and forgone profits.[276] Consequently, under the Law on Information, to collect damages for the interference with right to access or disclose information, one needed to present considerable proof; this made remedy nearly impossible.

In 1993, the legislature amended the Ukranian Civil Code adding the moral harm provision, which allowed for the filing of damages for mental suffering.[277] It is difficult to say whether this provision has ever been used to promote an individual's right to information. Neither the press nor statistics provide any proof to this effect. However, evidence that public officials use this new democratic concept to suppress freedom of speech is now widely known and discussed. Officials turned the moral harm concept

271. GIPI, *supra* note 241.

272. Schauer, *supra* note 227, at 272.

273. Douglass C. North, *The New Institutional Economics and Development* 5 (Washington University in St. Louis, working paper Sept. 8, 1993), *available at* http://econwpa.wustl.edu:8089/epseh/papers/9309/9309002.pdf (last visited Feb. 9, 2004).

274. Stephen J. Toope, *Legal and Judicial Reform through Development Assistance: Some Lessons*, 48 MCGILL L.J. 357, 371 (2003).

275. Law on Information, *supra* note 30, arts. 48, 49.

276. KRASAVCHIKOV, *supra* note 91, at 423.

277. Ukr. Civ. Code arts. 440–444.

into a mechanism limiting freedom of information by filing defamation suits against the media criticizing its conduct.

Some of the awards that officials obtained from the courts are dramatic even by western standards. For example, a member of a city council obtained a judgment for over 143,000 USD when local media publicized facts from his prior criminal past.[278] In an even more prominent case, Minister of the Interior, Y. Kravchenko, obtained a judgment for over 2.5 million USD from a newspaper that had accused him of abusing his office.[279] Such developments astonished the European human rights world with reversal of the legal norm. In the eyes of the Council of Europe, defamation suits became an impermissible constraint on the freedom of information. In 2001, the Monitoring Commission of the Parliamentary Assembly even considered excluding Ukraine from the Council.[280]

It took years of lobbying by local interest groups, coupled with threats by the international community, to convince the legislation to balance this accidental anti-democratic shift. In April 2003, the Parliament finally adopted the Law on Amendment of Some Legislative Acts of the Ukraine on Issues of Ensuring an Unimpeded Realization of a Human Right to Freedom of Speech.[281] This statute provided that "[a] person shall be released from liability for dissemination of information with restricted access (e.g., personal data) if the court establishes that this information is socially important."[282] This provision, along with several others, may help to strike a better balance between privacy and information rights in today's Ukraine.

However, there is still a strong cultural tendency to restrict private actors' liberty to publish and acquire information. For example, the 2004 Civil Code dedicates only one article to the right to information,[283] but commits at least ten articles to privacy.[284] Moreover, the articles on privacy are quite strict. For example, according to the Code, in order to

278. KHRG, *supra* note 35, at 19.

279. *See, e.g.*, Human Rights Watch, Ukraine Negotiating the News: Informal State Censorship of Ukrainian Television, No. 2(D) at 11 (2003), *available at* http://www.hrw.org/reports/2003/ukraine0303/Ukraine0303.pdf (last visited Jan. 6, 2006).

280. EUR. PARL. ASS., ON FREEDOM OF EXPRESSION AND THE FUNCTIONING OF PARLIAMENTARY DEMOCRACY IN UKRAINE, RECOMMENDATION 1497 (Jan. 25, 2001).

281. Zakon Ukrajiny pro Vnesenn'a Zmin do Dejakykh Zakonodavchykh Active Ukrajiny z Pytan' Zabezpechenn'a ta Bezpereshkodnoji Realizatsiji Prava L'udyny na Svobodu Slova [Law of Ukraine on Amendment of Some Legislative Acts of Ukraine on Issues of Ensuring and Unimpeded Realization of a Human Right to Freedom of Speech] #676-IV (Apr. 3, 2003) (author's trans.) (on file with author).

282. *Id.* § 2 (1).

283. Ukr. Civ. Code art. 302.

284. *Id.* arts. 286, 294–96, 299, 301–03, 306–08.

publish a correspondence, one must obtain consent from the addressor, the addressee, and from all third persons mentioned by name in the correspondence.[285] A new law on data protection under such circumstances is likely to cause a further shift away from freedom of information.

A bill currently in Parliament supports the existence of this threat to freedom of information. The bill not only prohibits the collection of personal data without consent, but also requires that the consent be in writing.[286] The drafters attempt to strike a balance in favor of freedom of information, but their attempt seems weak. Unlike the EU General Directive, which is structured to provide detailed exceptions immediately following each restriction, the Ukrainian lawmakers suggest a single general phrase at the end. The lawmakers propose that the right to privacy of personal data may be restricted "in the interest of . . . national, economical, and public safety or for . . . protection of human rights."[287] Unlike the European system, the Ukrainian bill does not privilege journalists, direct marketers, or any other business professionals closely connected with processing personal data.[288] Although harmonization with European legislation is cited as a primary justification for promoting the bill,[289] interest groups already have expressed significant concern that the bill is merely a restriction of the right to self-expression.[290]

Ukraine's deeply entrenched Soviet legacy may turn a new data protection statute into a modernized tool for suppressing, rather than balancing, freedom of speech. Perhaps the Ukrainian cultural tradition is closer to European socialism than to American capitalism. This tradition likely makes both data subjects and data controllers more comfortable with centralized governmental regulation than with a dispersed industry-standard setting. However, this potential comfort with governmental regulation is the very factor that presents a threat. In order to ensure the effectiveness of a data protection statute, Ukraine will need to restructure its institutional framework to provide better safeguards for fair creation

285. *Id.* art. 306.

286. Bill on Data Protection, *supra* note 92, art. 5.

287. *Id.* art. 29.

288. GIPI, *supra* note 241.

289. M. Scherbat'uk, *Komentar do Zakonoproektu "Pro Zakhyst Personal'nykh Danykh"* [*A Comment on the Draft Law On Protection of Personal Data*], http://ilaw.org.ua/comments_bill.php?id=12 (last visited Jan. 24, 2006) (author's trans.) [hereinafter Scherbat'uk].

290. *See id.*; *see also* Kashpur, *supra* note 257; and T. Shevchenko, *U Rozrizi Dyskusiji navkolo Proektu Zakonu Ukrajiny "Pro Zakhyst Personal'nykh Danykh"* [*In Context of Discussion Around Draft Law of Ukraine on Protection of Personal Data*], *available at* http://ilaw.org.ua/comments_bill.php?id=12 (last visited Jan. 24, 2006) (author's trans.).

and interpretation of the law. This cost of transition is high. In the meantime, if Ukraine does not want to pay it, will the European be affected? Can the lack of a data protection statute lead to a loss of business with the European Union?

3. Costs of Non-Transition for the Balancing of the Interest in Data Protection Against the Interest in Free Flow of Information

A closer look into the nature of business restrictions potentially derived from inadequate data protection proves that the risk is negligible. Formal accession of Ukraine to the EU is unlikely to occur in the near future. For advancement of informal integration—the boosting of flow of goods, services, people, and capital—there is no guarantee that the statute will make a difference.

In determining the adequacy of the data protection system in each country, the European authorities give great deference not only to the written law, but also to procedural and enforcement mechanisms including ensuring a good level of compliance with the rules, providing support and help to individual data subjects in the exercise of their rights, and providing appropriate redress to injured parties when rules are violated.[291] According to the EU, the countries with Adequacy Status regarding data protection currently are limited to Switzerland, Canada, Argentina, and Guernsey. The U.S. system is deemed adequate only insofar as a transfer of data is covered by a Safe Harbor or a Passenger Air Transfer Agreement.[292] Even if Ukraine invests all of its political power into an attempt to achieve EU Adequacy Status, the process will take the EU at least a few years.[293]

In addition to being extremely difficult to achieve, Adequacy Status likely will bring no special advantages. A negligible number of European businesses today export data outside the EU. European Commission surveys prove that only one in ten companies transfers personal data outside the EU or the European Economic Area (EEA).[294] Even if the need for transborder data flow becomes more important in future partnerships, there are a number of ways to secure adequate protection of the EU-originated data in Ukraine even in the absence of comprehensive

---

291. KUNER, *supra* note 104, at 134.

292. *See* EUROPA, Justice and Home Affairs—Data Protection, Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, http:/europa.eu.int/comm/justic_home/fsj/privacy/thridcountries/index_en.htm (last visited Feb. 2, 2006).

293. KUNER, *supra* note 104, at 136.

294. *Eurobarometer*, *supra* note 139, at 5.

legislation. Recognizing the need to promote transborder data flows, the General Directive sets forth several alternatives, including model contract clauses, adequate safeguards in particular ad hoc contracts, codes of conduct, and others.[295] Finally, while development of business relations with the EU hardly depends greatly on the adoption of a data protection statute, business relations with the United States likely would suffer from such adoption, discouraging laissez-faire oriented U.S. companies from seeking the Ukrainian market.

V. CONCLUSION

Under Soviet rule, it was believed that time would lessen the need for laws. The fall of the Soviet Union and the desire to enter the EU have strengthened the notion of rule of law in Ukraine. Accordingly, adoption of an omnibus statute for the legal system to address a novel data protection problem appears to offer the most appropriate solution for Ukraine. As the European experience suggests, a statute could establish data protection as an important social value, articulate data processing rules, and fairly balance the competing interests of privacy and free flow of information. However, a statute alone does not guarantee enforced law. In a society with no legacy of democratic institutions, where no demand yet exists for such law, and which lacks basic enforcement resources, the cost of creating an effective law will be high. Unable to pay this cost, the nation may simply reframe Soviet-style censorship into a new human-rights-shaped mold.

In light of Ukraine's social history and goal of entering the EU, the U.S. model may be unsuitable for the country to follow in the long term. However, for the short term, self-regulation in Ukraine can provide a safe harbor against revolutionary change. It can channel an under resourced governmental effort into, more urgent areas of building a democracy, such as fostering maturation of demand for information privacy, and helping data-processing businesses rise to their feet. Self-regulation will encourage businesses in Ukraine to learn directly from newly-acquired western partners the most appropriate practices of data processing. Private experience will fertilize the soil for planting a viable statute, if needed, when the time comes.

---

295. KUNER, *supra* note 104, at 124.