Privacy–An Endless Debate?

Spiros Simitis†

I.
PRIVACY

In August 1960 William L. Prosser published a remarkable analysis of privacy in the *California Law Review*.[1] Prosser addressed the privacy tort's increasing complexity, its myriad purposes, and its transformation into an overly broad scheme of liability. Responding to these issues, Prosser proposed four distinct privacy torts: the intrusion upon the plaintiff's solitude, a public disclosure of embarrassing facts, a public distortion of the plaintiff's public image, and an appropriation of the plaintiff's specific characteristics.[2]

Prosser analyzed privacy against the background of American experiences. Consequently, his views were shaped by the American legislative and judicial context. But none of the developments Prosser described is a singularly American phenomenon. Prosser's reference to Warren and Brandeis's 1890 article in the *Harvard Law Review*[3] could just as easily have been expanded with references to German cases concerned with the "right to be left alone."

† Professor of Law, Director, Research Center for Data Protection, Goethe University, Frankfurt-am-Main, Germany. Member, German Bioethics Commission.

1. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).
2. *Id.* at 389.
3. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Thus, similar privacy concerns are expressed in decisions of the Reichsgericht, the German Supreme Court, in the 1920s. In those cases, irrespective of whether the plaintiff was the President of the German Republic,[4] its Defense Minister,[5] the Count Friedrich von Zeppelin ("father" of the first large dirigible airship),[6] or a less prominent person, the Court focused, as in the United States, on the right "to be let alone."[7]

Moreover, the cause was identical in Germany and the United States. In both countries, a concern for privacy was spurred by the rapid expansion of mass media. In the United States, Warren and Brandeis's famous article addressed this issue, and in Germany, the equally well-known cases of Friedrich Ebert and Gustav Noske confronted the same questions. Once more, the media's activities demand that privacy be acknowledged and respected. Prosser's definition of the privacy torts and the comparable efforts in Germany to identify the applicable rules are all responses to the far-reaching repercussions of a communication process increasingly dominated by mass media.

II.
THE RIGHT TO PRIVACY IN GERMANY AND THE EUROPEAN UNION

A. The Right to Privacy in Germany

Despite Warren and Brandeis's emphatic pleas for privacy and the nearly simultaneous requests of Gareis[8] and von Gierke[9] to protect privacy,[10] the resistance to privacy proved fiercer in Germany than in the United States.

The German Civil Code's basic provision for tort liability, section 823, paragraph 1, starts by addressing the infringement of enumerated rights such as property, health, or freedom. But the paragraph closes with a general reference to "other rights." Therefore, all the Courts needed to do was to simply extend the "other rights" concept to include privacy. Instead an openly negative reaction prevailed for mainly two reasons. First, the Courts wanted to avoid judgments that could be perceived as ignoring the legislature's decision. The German legislature had indeed expressly rejected all attempts to join the Swiss pioneer efforts (section 28 of the Civil Code) in unequivocally guaranteeing

4. Reichsgericht, 25 DEUTSCHE JURISTEN-ZEITUNG 596 (1920).
5. *Id.*
6. Reichsgericht, RGZ 74, 311 – Entscheidungen in Zivilsachen (1911).
7. THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888).
8. Karl Gareis, *Die Privatrechtssphäre im modernen Kulturstaate*, 3 GESETZGEBUNG UND PRAXIS AUF DEM GEBIET DES DEUTSCHEN ÖFFENTLICHEN RECHTS 137 (1877).
9. 1 OTTO VON GIERKE, DEUTSCHES PRIVATRECHT 703 (1895).
10. *See also* Diethelm Klippel, *Historische Wurzeln und Funktionen von Immaterialgüter- und Persönlichkeitsrechten im 19. Jahrhundert*, 4 ZEITSCHRIFT FÜR NEUERE RECHTSGESCHICHTE 132 (1982).

privacy.[11] Consequently, in the eyes of most justices, to read the "protection of personality" into section 823, paragraph 1, would overtly bypass the legislature's intent. Second, privacy cases often involved important political leaders such as the President of the Republic and the Defense Minister. The Courts did not want to step into a politically charged discourse, particularly given a regime as unstable and distrusted as the Weimar Republic.

Nonetheless, despite their refusal to openly correct the lack of a tort-based privacy protection, the Justices hoped to craft a solution that would allow them to shape the law on their terms. Hence, they formally relied on the two explicit instances in which the legislature had indeed permitted a privacy defense: "name"[12] and "picture,"[13] both understood as essential characteristics of a "life-picture."[14] In some cases the Justices also sought refuge in the general duty to compensate for damages caused by offending good morals.[15] Thus, instead of finding a simple privacy right, a more complicated path was taken by relying on these potential reference points in order to justify judicial interventions. However, these interventions hardly coped with the mass media's growing influence.

The initial approach was due to a growing recognition of the need to assert political and legal principles that ensure the individual's dignity in a democratic society that changed radically in the 1950s. In May 1954 the Bundesgerichtshof, the German Federal Supreme Court,[16] ordered a weekly newspaper to republish in its news pages a letter, parts of which had originally been brought in the "Letters to the editor," that corrected an error regarding a newly established bank. The Court justified its decision through a direct reference to the constitutionally guaranteed duty to respect the claimant's dignity[17] and to not infringe a free development of his person.[18] Thus, the Federal Supreme Court clearly redefined the perception of privacy and settled the acknowledgment of "a right of personality." Moreover, the Court indicated that any changes to privacy protection must comply with Articles 1 and 2 of the

11. *See, e.g.*, 1 PROTOKOLLE DER KOMMISSION FÜR DIE ZWEITE LESUNG DES BÜRGERLICHEN GESETZBUCHS 822 (1897). *But see* Helmut Coing, *Zur Entwicklung des zivilrechtlichen Persönlichkeitsschutzes*, JURISTENZEITUNG 558 (1958); Mario M. Pedrazzini, *Helvetische Glossen zum Persönlichkeitsrecht*, *in* FESTSCHRIFT FÜR KLEMENS PLEYER ZUM 65. GEBURTSTAG 567 (Paul Hofmann ed., 1976).

12. BÜRGERLICHES GESETZBUCH [BGB] [Civil Code], Jan. 1, 1900, RGBL. 1896 at 195, § 12 (Ger.).

13. Kunsturhebergesetz [KUG] [Act on the Protection of the Copyright in Works of Art and Photographs], Jan. 15, 1907, BGBL. III/FNA at 440–43, § 23 (Ger.).

14. *See* Rudolf Reinhardt, *Das „Lebensbild" und der Schutz der Persönlichkeit im modernen Privatrecht*, *in* PERSÖNLICHKEIT IN DER DEMOKRATIE – FESTSCHRIFT FÜR ERICH SCHWINGE ZUM 70. GEBURTSTAG 127 (Hans U. Evers ed., 1973).

15. Bürgerliches Gesetzbuch [Civil Code] § 826.

16. Federal Supreme Court, BGHZ 13 (334) (1954).

17. BUNDESVERFASSUNG [BV] [CONSTITUTION], art. 1, para. 1 (Ger.).

18. *Id.*, art. 2 para. 1.

Constitution.

In an equally path-breaking judgment, the Bundesverfassungsgericht, the Federal Constitutional Court,[19] confirmed the Federal Supreme Court's opinion and clarified that the constitutional guarantee of privacy tolerates no distinctions between public authorities and private persons or institutions. Hence, a priori exemptions of specific areas or activities from privacy protection are as unconstitutional as the repeated attempts to distinguish between a direct application of constitutional principles in the public sector and an indirect relevance in the private sector. Experience has demonstrated that any such distinction ultimately deprives the constitutional principles of their effect.

In later judgments, both Courts have detailed the requirements of a right to privacy and, at the same time, adapted them to the demands of concrete conflicts.[20] Thus, for instance, the Constitutional Court has stated that though the freedom of the press may, particularly in the case of public figures, justify more limited protection, a minimum of clearly protective measures must still be taken.[21]

B. The Right to Privacy in the European Union

In 1950, the European Convention for the Protection of Human Rights (art. 8) already guaranteed to everyone the "right to respect for his private and family life, home and correspondence,"[22] and a formulation that was literally repeated thirty years later in the European Union's Charter on Fundamental Rights (art. 7).[23] However, like the Human Rights Convention, the Charter had no immediate practical effects. Therefore, the European Union's organs and institutions were only obliged to strictly comply with the Charter when the Lisbon Treaty came into force.[24]

But although the Charter and the Human Right's Convention share a common text, they are interpreted differently. For example, in the opinion of

---

19. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], BVerfGE 7, 198 (1958); BVerfGE 34, 269 (1973).

20. S*ee* Ernst von Caemmerer, *Der privatrechtliche Persönlichkeitsschutz nach deutschem Recht*, *in* FESTSCHRIFT FÜR FRITZ VON HIPPEL, 27 (Josef Esser ed., 1967); ERNST STEINDORFF, PERSÖNLICHKEITSSCHUTZ IM ZIVILRECHT (1983); DIETER GRIMM, *Persönlichkeitsschutz im Verfassungsrecht*, KARLSRUHER FORUM 1996 - SCHUTZ DER PERSÖNLICHKEIT 3 (1997); Peter Schwerdtner, *Persönlichkeitsrecht im Privatrecht*, KARLSRUHER FORUM 1996 - SCHUTZ DER PERSÖNLICHKEIT 28 (1997).

21. Federal Constitutional Court, 54 NJW 1921 (2001); *see also* Federal Supreme Court, BGHZ 128, 1 (1996).

22. Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, Rome 4.XI.1950, European Treaty Series [ETS] no. 5.

23. Charter of Fundamental Rights of the European Union, proclaimed by the European Council on December 7, 2000 in Nice, O.J., 18.12.2000, C 364/1.

24. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13 2007, 2007 O.J. (C 306) 1.

the European Court of Human Rights,[25] whenever freedom of press is at stake, article 8 of the Convention justifies diminished privacy protection if persons concerned are politicians, a view obviously accepted by the German Federal Constitutional Court.[26] Nonetheless, both documents affirm the change in the discussion's focal point. The discourse surrounding privacy rights has shifted from a tort-oriented approach to an understanding grounded in elementary constitutional principles that stresses the importance of effective safeguards, establishes a foundation for judicial decisions, and asserts the necessity of preventing and punishing intrusions on privacy.

As evident as the constitutionalization process within the European Union is, it does not justify a perception of privacy where, as in James Whitman's view, dignity concerns are weightier in Europe while liberty interests predominate in the United States.[27] The German Courts, as already mentioned, made a conscious choice to ground privacy in both concepts. Besides, precisely because of the importance of both dignity and liberty, the European Union and its Member States are obliged to protect privacy in both their internal regulations and external agreements.

In sum, since the Lisbon Treaty the European Union has no choice: privacy cannot be determined at will. The Union's considerations have always been grounded on article 7 as well as on all other privacy-relevant provisions of the Charter, in particular article 8. Consequently, contrary to the arguments of some scholars, the European Union neither acts against the background of an "antiquated" Privacy Directive of the European Commission, nor intends to impose its views on the rest of the world as a kind of "privacy cop,"[28] but merely follows the Charter and the duties imposed on it there.

III.
THE UNEASY STATUS OF PRIVACY RIGHTS

The extension of constitutional rights to privacy emphasizes the importance of an efficient protection. Nevertheless it does not clarify the protection's precise scope. In fact, the more stronger privacy safeguards were demanded, the more difficult it became to find agreement on the modalities of an adequate protection.

Controversies as those in Germany over the monitoring, by police and other public authorities in the security sector, of conversations in private homes

25. European Court of Human Rights, Von Hannover v. Germany, 294 Eur. Ct. H.R. (2004).

26. *See* BVerfGE, 101, 361,392 (2000).

27. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

28. Justin Santolli, *Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive*, 40 GEO. WASH. INT'L. L. REV. 553 (2008).

are a typical example. An initial attempt to install the necessary devices throughout a particular private home was abandoned because of the repeated references in the German Federal Constitutional Court's decisions to an inviolable core of the private sphere.[29] Instead, an exception for the bedroom, and possibly one or two other rooms, was envisaged but quickly abandoned. The risk that such exceptions could jeopardize the gathering of needed information by placing certain rooms in residences "off limits" to surveillance was far too obvious. Therefore, preference was given to techniques that permit the monitoring of all conversations in the home from outside, despite their hardly deniable incompatibility with the Federal Constitutional Court's jurisprudence. Nonetheless the weakness of all still ongoing efforts to postulate an impenetrable and thus indisputably "intimate" sphere could hardly have been better demonstrated.

The growing relevance of the constitutional aspects of privacy did not only strengthen privacy protection. It also set off conflicts such as those between privacy and freedom of the press.[30] While German law confirms the duty to secure the best possible privacy protection for persons concerned, freedom of the press generally prevails over privacy in the United States. The Wikipedia case is a recent illustration of the diverging approach.[31] In 1990, two people killed Walter Sedlmayr, an actor, and were sent to jail. They were released from prison in 2007 and 2008 and almost immediately tried to have their names removed from prior publications and to prohibit any further reference to their past. "They should," as their lawyer said, be rehabilitated and "lead their life without being publicly stigmatized."[32] For exactly this reason, the editors of Wikipedia's German-version deleted all mention of the two men in an article about Walter Sedlmayr. Both of them have also sued the Wikipedia Foundation to have their names removed from the English-language version. In the United States, the reaction thus far has been rather disinterested comments such as the lapidary remark that every Justice on the United States Supreme Court would agree that the Wikipedia article "is easily, comfortably protected by the First Amendment."[33]

IV.

29. *See, e.g.*, Federal Constitutional Court, BVerfGE 120, 274, 335 (2008); BVerfGE 106, 28, 39 (2003); BVerfGE 80, 367, 376 (1990); BVerfGE 73, 118 (1987); BVerfGE 34, 238, 247 (1973).

30. *See also supra* notes 21, 25.

31. *See, e.g.*, John Schwartz, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, N.Y. TIMES, Nov. 13, 2009, at A13; Evgeny Morozov, *Free Speech and the Internet*, INT'L HERALD TRIB., Nov. 28, 2009, at 8.

32. *See* Schwartz, *supra* note 31.

33. *Id.*

DATA PROTECTION

William Prosser's 1960 article was far more a critical look back than a guideline for future reflections on privacy. His key point had already been mentioned in publications of Wiener[34] and Frank,[35] which saluted "cybernetic machines" as guarantees of an unprecedented rationalization of social and political discourse. Their central statement was that never before had it been possible to collect and process a virtually unlimited amount of information, and therefore the chances of truly objective decisions had never been so good. Consequently the rapidly expanding use of "machines" was regarded as the passage to communication structures guided by a thorough and transparent analysis of all relevant information. In the future, decisions about individuals would no longer be based on speculations or influenced by a purely subjective approach.

Databanks, like the collection initiated by the Government of the German Federal State of Hesse in the middle of the 1960s,[36] embodied the hopes evoked by "cybernetic machines." The data collections were to allow efficient long-term policies, such as in finance and social security, and also to secure better medical help, especially in emergencies. But while the databanks were at first generally accepted, doubts gradually arose, beginning in 1968, with regard to the processing of personal data. The involvement of nearly all Hesse citizens, the storage of especially sensitive data, as those concerning health or income, and the databank's capacity to exploit information for different purposes triggered demands that the Government investigate the risks of a permanent surveillance of citizens. As a consequence, on October 10, 1970, the Hessian Parliament adopted the world's first Data Protection Act after a short but intensive debate.[37]

The adoption of the Hessian Act was preceded by a careful study of similar expectations especially in the United States, the clearly prevailing information source at that time. Congressional hearings on "Computer and Invasion of Privacy,"[38] "Commercial Credit Bureaus,"[39] and "Computer

34. NORBERT WIENER, CYBERNETICS: OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (2d. ed. 1961).

35. KYBERNETISCHE MASCHINEN (Helmar G. Frank ed., 1964).

36. S*ee* HESSISCHE ZENTRALE FÜR DATENVERARBEITUNG, GROSSER HESSENPLAN: ENTWICKLUNGSPROGRAMM FÜR DEN AUSBAU DER DATENVERARBEITUNG IN HESSEN (1970).

37. Hessisches Datenschutzgesetz [HDSG] [Hessian Data Protection Act], Hess GVBl. I 625 (1970). For its history, see Spiros Simitis, *Zwanzig Jahre Datenschutz in Hessen – eine kritische Bilanz*, *in* 19 TÄTIGKEITSBERICHT DES HESSISCHEN DATENSCHUTZBEAUFTRAGTEN 138 (1990).

38. *Hearings on the Computer and Invasion of Privacy Before the H. Spec. Subcomm. on Invasion of Privacy of the H. Comm. on Gov't Operations*, 89th Cong. (1966).

39. *Hearings on Commercial Credit Bureaus Before the H. Spec. Subcomm. on Invasion of Privacy of the H. Comm. on Gov't Operations*, 90th Cong. (1968).

Privacy,"[40] as well as the congressional report on "Privacy and the National Data Bank Concept,"[41] and the contributions to the growing debate in law and social sciences about privacy protection in an ever more computerized age,[42] were among the documents consulted.

The Hessian Act was followed by the adoption of data protection laws in other countries, beginning with Sweden in 1973 and provisionally ending with Mexico in 2010. A common characteristic of nearly all these laws is their omnibus approach. In other words, they all contain rules applicable to every kind of processing of personal data. An approach like this openly contrasts with the prevalence of sectoral-oriented provisions[43] in the United States.[44] Clearly sectoral rules depart from an omnibus regulation approach and instead deliberately focus on a specific context of data processing, such as credit reporting, information collected for insurance purposes, or the processing of personal data by the police as well as the various health agencies.

The Hessian Parliament's nearly unanimous and astonishingly quick enactment of the Data Protection Act was due, in part, to the limited scope of the Act—it addressed only the public sector's automated processing of personal data. In contrast, whenever rules regarding private persons and businesses were considered, the result was a remarkable delay, mainly caused by demands for a more lenient regulation of the private sector, long supported by the assertion that private entities would never have the financial or technical means needed to establish databanks as large and comprehensive as those of government. Thus, the German Federal Data Protection Law was passed only after five years of intense controversies shaped by the requests to mitigate the duties of private data processors.[45] To this day, the law's provisions still reflect the efforts to exclude private data processors from strict regulations addressing essential elements of a reliable protection. While, for instance, truly independent controllers oversee public entities, the private sector is inspected by agencies subject to government directives, a distinction that has been clearly rejected by the European Court of Justice[46] as utterly incompatible with the independence

40. *Hearings on Computer Privacy Before the H. Subcomm. on Administrative Practice and Procedure of the H. Comm. on the Judiciary*, 90th Cong. (1968).

41. H. COMM ON GOV'T OPERATIONS, PRIVACY AND THE NATIONAL DATA BANK CONCEPT, H.R. REP. NO. 1842 (1968).

42. *See, e.g.*, Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969); ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

43. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 908 (2009).

44. *See id.* at 922, 931; Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009). The one American exception to this sectoral approach is the 1974 Privacy Act, 5 U.S.C. § 552a (2000).

45. Bundesdatenschutzgesetz [BDSG] [Data Protection Act], Feb. 1, 1977, BGBL. I 201.

46. European Court of Justice (Grand Chamber), Case C-518/07 European Commission supported by the European Data Protection Supervisor v. Federal Republic of Germany, 2010

explicitly required by the European Data Protection Directive.[47]

Comparable controversies accompanied the history of the 1995 European Data Protection Directive,[48] as once more there were tenacious attempts to eliminate or at least weaken an independent external control of data processors. There has also been a virtually indefinite postponement of the long overdue review of the Directive. Thirty-five years after its adoption the Directive's provisions need more than ever to be adapted to the changes in technology as well as to the experiences on both the national and supranational levels.[49]

German data protection laws were at first grounded in exactly the same articles of the Constitution that generally guarantee privacy protection.[50] Nonetheless, the Federal Constitutional Court redefined the conditions of access to personal data in a seminal judgment in 1983 that involved a routine census with equally routine questions.[51] In response to the government's census-plans, there had been a spontaneous and unprecedented public protest. The planned collection of detailed information on every person and the intended systematic use of computerized processing were seen as unmistakable signs of a government policy aimed at limitless surveillance and manipulation of its citizens.[52]

In its "Census" opinion, the Constitutional Court stated that the duty to respect the individual's dignity and his freedom to develop his personality must, especially in view of technologies allowing a processing of an ever greater amount of personal data, be complemented by a "right to informational self-determination."[53] Individuals should, in other words, have the right to determine who can use their data, for what purpose, on what conditions, and for how long.[54] Only then, the Court added, would individuals be able to freely form, express, and defend their opinions. The Court concluded that the more personal privacy is curtailed, the more individuals will gradually give up their constitutional rights. Informational self-determination, the Court stated, must therefore be seen and treated as an elementary precondition of a democratic

---

E.C.R. I-00000.

47. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 28 para. 1, 1995 O.J. (L 281).

48. *Id.*

49. *See* Spiros Simitis, *Die EG-Datenschutzrichtlinie: eine überfällige Reformaufgabe*, *in* FESTSCHRIFT FÜR WINFRIED HASSEMER ZUM 70. GEBURTSTAG 1235 (Felix Herzog & Ulfried Neumann ed., 2010).

50. *See supra* notes 18, 19.

51. Federal Constitutional Court, BVerfGE 65, 1 (1984).

52. For a discussion in English, see Paul M. Schwartz, *The Computer in German and American Constitutional Law*, 37 AM. J. COMP. LAW 675 (1989).

53. Federal Constitutional Court, BVerfGE 65, 1, 43 (1984).

54. For an English excerpt from the opinion, see DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 323–26 (2d ed. 1997).

society.[55] Both its existence and functioning depend, thus, on the capacity of citizens to autonomously act and participate in society, a capability irrevocably linked to the knowledge and control of their personal data.

Since then, the Court has, on several occasions, underscored the importance of informational self-determination and affirmed that the legislature may foresee exceptions, but only in precisely defined cases, for clearly indicated purposes, and for accurately described and reliably controllable conditions of data use.[56] In fact, in 2010 the Constitutional Court struck down a statute that required a preventive storage of every person's telecommunication data in order to better combat severe forms of crime.[57]

Moreover, in 2008, the Court expanded the "informational self-determination" by a "guarantee of confidentiality and integrity of technical information systems."[58] This right protects against a secret infiltration of technical information systems, and is, in particular, directed against the government's security agencies. Exceptions are permitted only in cases in which particularly important legal interests, such as the life and freedom of persons concerned or the existence of the State, are concretely endangered. As an additional safeguard, a court must, as a rule, first authorize the infiltration.

Using "informational self-determination" as a prerequisite of a democratic society confirms the central role of the individual, but it does not confer on individuals a limitless power of decision-making. Most data protection laws may still begin by categorically asserting that processing of personal data can be either justified by the data subject's consent or by an explicit legal regulation. Nevertheless, neither the data subject's particular situation nor the specific context of the consent can be ignored. Consequently, labor courts in Germany[59] and elsewhere[60] have, because of employees' inherently uneven bargaining power, steadily restricted the questions that employers can ask of employees and the data that can be collected about them. Quite on the same lines, the International Labour Office (ILO) opted for carefully differentiated rules in its Code on the Protection of Worker's Personal Data.[61] Thus, for

55. Federal Constitutional Court, BVerfGE 65, 1, 43 (1984)

56. *Id.* at 43–46; *see also* BVerfGE 120, 274 (2008); BVerfGE 103, 21 (2000); BVerfGE 93, 181 (1995); BVerfGE 84, 192 (1991); BVerfGE 78, 77 (1988).

57. Federal Constitutional Court, 63 NJW 833 (2010).

58. Federal Constitutional Court, BVerfGE 120, 274 (2008).

59. *See, e.g.*, Bundesarbeitsgericht [BAG] [Federal Labor Court], Federal Labor Court, 2 NZA 848 (2003) (pregnancy); Federal Labor Court, 2 NZA 57 (1985) (corporal handicaps); Federal Labor Court, 39 BETRIEBS - BERATER 533 (1984) (wages by former employers).

60. See, especially, judgments of the European Court of Justice reviewing national regulation reviewing national regulation. *See, e.g.*, Case C-13/94, P. v. S. & Cornwall Cnty. Council, 1996 E.C.R. I-2143 (U.K.); Case C-207/98, Silke-Karin Mahlburg v. Land Mecklenburg-Vorpommern, 1998 E.C.R. I-549 (Ger.); Case C-109/00, Tele Danmark, 2001 E.C.R. I-06993 (Denmark).

61. INT'L LABOUR OFFICE, PROTECTION OF WORKERS' PERSONAL DATA: AN ILO CODE OF

example, genetic screening should be generally prohibited, subject to possible exceptions explicitly indicated by national laws (art. 6.12). As with labor relations, experiences in the credit area have consistently shown that a transfer of data concerning borrowers to third parties must be restricted to a few necessary cases. The German legislature tried to at least partially reach this result in the latest amendments to the Federal Data Protection Act.[62]

Thus, labor relations and credit policies illustrate that informational self-determination presupposes definitely more than the mere abstract acceptance of everyone's right to define the use of his or her data. The ability to influence the processing depends on its particular context. Therefore, only as long as the respect of every person's right is also understood as a duty to always consider the context of the processing can self-determination be guaranteed while also yielding to the exigencies of a democratic society.

Another equally relevant example of the need to consider the close relationship between data protection and a democratic society is the expanding commercialization of personal data. It has been justified as a perfectly normal result of either the data subject's property right,[63] or more specifically, the subject's right to determine the use of his or her data. But although both these approaches recognize that information processing implies a range of economic interests, they ignore the full social costs of data use.[64]

The more people consent to the commercial use of their data by a particular business, the more they are integrated into a system that improves the firm's chances to influence their behavior. Firms exploit this influence over people's behavior primarily to further their own interests and future plans. Therefore, the commercialization initiates and furthers a long-term manipulation of the data subjects and must be for precisely this reason measured against the demands of a functioning democratic society.

Data protection laws have always been marked by the uneasiness in dealing with constantly advancing technology. Legislators deliberately chose a distinctly abstract language in order to improve the chances to address unknown aspects and new developments of technology. Nevertheless, the more computers expanded, the clearer it became that the original rules had to be replaced by regulations that explicitly took specific uses into account. Pensions,

---

PRACTICE (1997).

62. Bundesdatenschutzgesetz § 28a(2) [BDSG] [Data Protection Act], July 29, 2009, BGBL. I 2254.

63. *See, e.g.*, Richard A. Posner, *An Economic Theory of Privacy*, 2 REGULATION 19 (1978); Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008); Thilo Weichert, *Zur Ökonomisierung des Rechts auf informationelle Selbstbestimmung*, *in* E-PRIVACY: DATENSCHUTZ IM INTERNET 158 (Helmut Bäumler ed., 2000); Wolfgang Kilian, *Informationelle Selbstbestimmung und Markprozess*e, 23 CR 921 (2002).

64. *See* Spiros Simitis, *Datenschutz – Rückschritt oder Neubeginn?*, 51 NJW 2473, 2477 (1998). *But see* RÜDIGER KLÜBER, PERSÖNLICHKEITSSCHUTZ UND KOMMERZIALISIERUNG (2007).

medical treatments, archives, tax records, insurance records, police reports necessarily contain personal data. An effective treatment of their processing substantially depends on the particular frame in which they fit. Hence, a well functioning protection presupposes provisions reacting to the risks of the concrete use.

As a result, lawmakers—especially in Europe—have enacted a second context-oriented generation of data protection regulations. Clearly sectoral laws are, for instance, increasingly used to regulate particularly sensitive processing areas. Statutes, such as those related to social security, preventive medical examinations, various security agencies, handicapped persons, or electronic health cards, include provisions on access to personal data. Europe more and more resembles the United States.[65] Omnibus laws were since the earliest days of data protection, especially in Europe, considered to be the only means to secure both a broad and reliable way to regulate the use of personal data. By now, a mounting and interminable amount of provisions dominates, an experience equally typical for the European Community, as the considerable number of Directives demonstrates.[66]

However, the assumption that the concentration on a particular context would ameliorate the protection of data subjects has been largely disproved. The sectoral approach is again and again seen by data controllers as an opportunity to limit the restrictions of the intended use. New processing rules in the law enforcement sector are characteristic of such a policy. A further example is Germany's newly established register of data related to labor relations.[67] An exceptional amount of information concerning an individual's former and actual employments, including data on "faulty comportment," that may very well be exploited for purposes such as profiling and evaluating potential employees, is systematically stored.[68] An official list as this register

65. *See* Schwartz, *supra* note 43, at 913, 931.

66. *See, e.g.*, Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Electronic Commerce in the Internal Market, 2000 O.J. (L 178) 1; Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 on the Processing of Personal Data and the Protection of the Privacy in Electronic Communication Sector, 2002 O.J. (L 201), 37, *modified by* Directive 2006/24 of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and amending Directive 2002/58/EC, art. 11, 2006 O.J. (L 105) 54; Directive 2003/98 of the European Parliament and of the Council of 17 November 2003 on the Re-use of Public Sector Information, 2003 O.J. (L 345), 90; Directive 2006/24 of the European Parliament and the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly available Electronic Communication Services or of Public Communications Network and amending Directive 2002/58/EC, 2006 O.J. (L 105), 54.

67. Gesetz über das Verfahren des elektronischen Entgeltnachweises [ELENA-Verfahrensgesetz] [Act on the Procedure of an Electronic Proof of Payments], Apr. 1, 2009, BGBL. I 634.

68. *See, e.g.*, Gunhil Lütge, *Elena, das Datenmonster*, DIE ZEIT, Mar. 18, 2010, at 26.

should never have been foreseen before definitively enumerating its purposes and exactly indicating the data that can be used for each of these objects. All the more, because data collections as those on the employees illustrate and underscore the crucial importance of a "right to forget"[69] or a "right to the silence of the chips."[70]

Experiences at the supranational level of the European Union (E.U.) are similar. The European Commission's explicitly stated willingness to comply with the European Charter of Fundamental Rights[71] has not stopped the Commission from adopting regulations that openly contravene its duty to restrict all data uses to information needed for a precisely determined purpose. Thus, an E.U. Directive[72] has legitimated even data collections that German law itself would otherwise prohibit.[73] In fact, the Commission itself has, just like some E.U. Member States, time after time disregarded, particularly in the security sector, basic demands of data protection. The attempt to conclude an agreement between the Union and the United States that would allow the United States to access financial data kept in Europe[74] and the Commission's Directorate General Internal Policies on a European Passenger Name Record System[75] are two recent examples of the Commission's inconsistent policies for privacy.[76]

In sum, there is a pressing need to thoroughly review regulatory approaches that, as in Europe, primarily rest on omnibus laws. Any further reflection should be guided by two requirements. First, legislators must limit themselves to the few core principles that every regulation of the use of personal data must observe. Second, all context-oriented rules must be conceived and applied as part of a uniform system based on a common foundation. Divergences may occur, but such exceptions should still fulfill two conditions:

---

69. David Reid, *France Ponders Right-to-Forget Law*, BBC, Jan. 8, 2010, http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm.

70. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Internet of Things–An Action Plan for Europe*, at 5COM (2009) 278 final (18.6.2009).

71. Daily Bulletin Europe, No. 7918. 8.3.2001, 7.

72. Directive 2006/24, *supra* note 64.

73. *See* Federal Constitutional Court, 63 NJW 833 (2010).

74. *Recommendation from the Commission to the Council to Authorise the Opening of Negotiations for an Agreement Between the European Union and the United States of America to Make Available to the United States Treasury Department Financial Messaging Data to Prevent and Combat Terrorism and Terrorist Financing (SWIFT)*, COM (2009) 703 final (Dec. 17, 2009).

75. Directorate General Internal Policies of the Union, Policy Department C Citizens' Rights and Constitutional Affairs, *Towards a European PNR System?*, PE 410.649 (Jan. 2009).

76. *See also* ARTICLE 29 DATA PROTECTION WORKING PARTY – WORKING GROUP ON POLICE AND JUSTICE, *The Future of Privacy*, Dec. 1, 2009, WP 168, a study of the Group entrusted in accordance with art. 29 of the 1995 European Commission's Data Protection Directive, *supra* note 46, with an independent counselling of the European Union on data protection issues. Spiros Simitis, *Der EuGH und die Vorratsdatenspeicherung oder die verfehlte Kehrtwende bei der Kompetenregelug*, 62 NJW 1782, 1783 (2009).

lawmakers should provide a specific justification for deviations, and should compensate any potential reduction in data protection with clearly defined measures. Thus, an exception from the common foundation would neither imperil the flexibility of the regulation nor the protection of personal data.

V.
THE ROAD AHEAD

The computerization of data use was initially seen, in both public and private sectors, as a means to help handle information pertinent to a specific issue, such as a criminal investigation, the cause and symptoms of certain diseases, or the administration of client data. However, the clearer it became that enhanced technology not only allows the processing of a practically endless amount of personal data but also an extendable linkage of data banks, the more the focus has shifted to preventive policies that in a growing number of cases initiate an intensive "predictive surveillance."[77]

Whether security issues, health problems, insurance, or marketing are at stake, data processing has become the foremost means for developing long-term strategies intended to disclose causalities, determine correctives, or steer and control a comportment that furthers the success of specific policy aims. Thus, for example, a British Biobank has been established to investigate diseases, such as Parkinson's, that are typical of an aging society.[78] As a result, information from about half a million persons, aged between forty-five and sixty-nine years, is now regularly collected in the United Kingdom. The Biobank includes medical and genetic data as well as information regarding family members, professional activities, specific preferences and habits, and social contacts. The constantly perfected profiles of registered persons have quickly led security agencies and insurance companies to express their interest in Biobank's data. While the regulation governing the activities of the Biobank finally denied insurance companies access, it explicitly permits security agency use.[79] Comparatively extensive collections were, for instance, discussed in France with regard to plans to diagnose cancer as early as possible and to link future insurance payments to patients strictly following a prescribed lifestyle.[80]

Both the European Commission and various E.U. Member States are also implementing regulations compelling private telecommunication companies to collect and store information potentially needed by security agencies in the

77. *See, e.g.*, Michael Lynch, *Predictive Surveillance: Precogs, CATCHEM, and DNA Databases*, 18 RISK & REG. 8 (Economic & Soc. Res. Council, London, U.K.) (Winter 2009).

78. *See* U.K. BIOBANK ETHICS AND GOVERNANCE COUNCIL, ANNUAL REVIEW (2006). *But see* GERMAN NATIONAL ETHICS COUNCIL, BIOBANKS FOR RESEARCH (2004).

79. *See* U.K. BIOBANK ETHICS AND GOVERNANCE COUNCIL, *supra* note 78, at 4.

80. *See, e.g.*, INSTITUT NATIONAL DE LA SANTÉ ET DE LA RECHERCHE MÉDICALE, TROUBLES DES CONDUITES CHEZ L'ENFANT ET L'ADOLESCENT (2005).

context of future criminal acts,[81] a striking change of data processing methods indeed. The government no longer sticks to the traditional direct collection of data. It turns instead to private entities. In doing so, the state not only acknowledges that the majority of data is stored in the private sector, but also establishes a processing model systematically combining information gathered in *both* public and private sectors. As a result, the government can limit its own gathering activities and opt for compelling services by businesses using data that might be of interest to public agencies.

However, this certainly noteworthy modification of the collection methods should not distract from the obvious violation of fundamental principles of data protection. In particular, the new approach disregards the emphatically proclaimed duty to only process data positively needed for a clearly defined purpose. The European Union's Charter of Fundamental Rights,[82] the European Commission's 1995 Data Protection Directive,[83] and the Data Protection Laws of the Member States all require concrete criminal acts or at least potential involvement of persons concerned, before personal data are collected.[84] Against this background, the German Federal Constitutional Court[85] unambiguously declared that the German law transposing the Data Retention Directive[86] to be unconstitutional and indirectly urged both the European Commission and the European Parliament to review the untenable Directive.[87]

Considerations about a review of the present data protection law are increasingly overshadowed by what may be the most significant challenge that a regulation of privacy has ever faced. As demonstrated daily by the spread of the Internet, technology has once again transformed the conditions of data use. Radically reassessed marketing strategies for consumer goods, countless chats criticizing products and services, widespread exchanges of experiences with physicians, detailed discussions about marital life, or a disclosure of every aspect of strictly personal habits, shifted data processing more and more to the Internet. In short, the Internet has redefined communication structures in a manner as radical as the introduction of computers. Nonetheless, legislators

81. *See supra* notes 57, 64.

82. *See supra* note 23, art. 8, para. 2.

83. *See supra* note 45, art. 6, para. 1.

84. *See, e.g.*, Bundesdatenschutzgesetz § 28a(2) [BDSG] [Data Protection Act], July 29, 2009, BGBL. I 2254.

85. Federal Constitutional Court, 63 NJW 833 (2010).

86. *Supra* note 66.

87. *See* Alexander Alvaro, *Positionspapier zur Einführung einer Vorratsspeicherung von Daten*, 21 RECHT DER DATENVERARBEITUNG [RDV] 47 (2005); Simitis, *supra* note 81, at 1783. The European Court of Justice ascertained in the case C-301/06, Ireland v. European Parliament & Council of the European Union, 2009 E.C.R. I-593, the European Commission's competence but strictly avoided to raise any questions concerning the Directive's content and its compatibility with the European Union's constitutional premises.

have to this day avoided a serious discourse regarding the implications of the Internet for data protection. The few attempts to address this issue concern especially criminal law and in particular child pornography. Openly negative reactions to privacy protection as well as a clearly temporizing attitude are obviously considerable, starting with the claim that the Internet is the first and only area of a truly unlimited free expression, continuing with references to numerous impediments due to the worldwide dimension of the Internet and a widespread hesitation resulting from an evident reluctance to harm the providers' interests. Nevertheless, legal principles, such as every person's right to determine the conditions of access to his or her data, or the right to be left alone, do not cease to be mandatory guidelines for all personal data uses. Conflicts like the assumedly open handling of information obtained from the Internet by employers on actual or potential employees demonstrate and confirm: the Internet must not be a law-free zone.

Providers have realized the pressing need for clear rules, but their primary choice is self-regulation,[88] as the case of Facebook reveals, despite its founder's assertion that social concerns about privacy are diminishing.[89] Hence, providers maintain a policy that permits them to safeguard their autonomy and avoid legislative scrutiny. Nonetheless, self-regulation does not suffice, as with automated data retrieval. In its opinion on informational self-determination, the German Federal Constitutional Court has purposely underscored the indispensability of mandatory legislative measures.[90] Self-regulation is not a genuine alternative to the legislature's intervention, even if, as with Facebook, users are fully informed and expressly asked to update their privacy settings. At best, self-regulation can help to supplement legislation.

Regulations addressing the use of personal information on the Internet appear, at first, perfectly normal extensions of generally accepted restrictions on data processing. However, their application would take place against the background of a unique experience: an unprecedented readiness to expose even the most private data. The same people who otherwise insist on the

88. *See Facebook Changes Privacy Policy*, BBC, Aug. 27, 2009, http://news.bbc.co.uk/2/hi/8225338.stm; *Facebook Gives Users More Control of Privacy*, BBC, Dec. 9, 2009, http://news.bbc.co.uk/2/hi/technology/8404284.stm; *Facebook Faces Criticism on Privacy Change*, BBC, Dec. 10, 2009, http://news.bbc.co.uk/2/hi/8405334.stm; Friederike Haupt, Sag mir, wo du stehst und wohin du gehst, FRANKFURTER ALLGEMEINE ZEITUNG, Mar. 20, 2010, at 42; Hendrik Wieduwilt, *Gesucht: Männlich, liiert, heterosexuell, aus Berlin*, FRANKFURTER ALLGEMEINE ZEITUNG, Dec. 22, 2009, at 19.

89. Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy is Over*, READWRITEWEB, Jan. 9, 2010, http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php. Mark Zuckerberg, the founder of Facebook, stated in an interview that "[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time." *Id.*

90. *See* note 51, at 44.

inaccessibility of their private sphere have evidently not the slightest hesitation to publicly revealing all its details. It is no wonder that social networking information, provided, for instance, by widespread flirting on Facebook, is now used in the United Kingdom as a divorce reason in every fifth divorce or separation case. An evaluation of chatting on the Internet has shown that it manifestly contributed to the proliferation of divorces in the last two years.[91] But the more the Internet is used to circulate and access strictly personal information, the clearer the question arises: Can a legally guaranteed respect for privacy be upheld in a society in which technology incites and sustains a constant disclosure of highly private data?

Despite these developments, however, privacy must remain a fundamental right in a society grounded on respect for the individual's personality. Consequently, reflections on the implications of profoundly modified conditions of communication are required more than ever before. Fifty years after the publication of William Prosser's article, the necessity to define and ensure the constitutive elements of privacy is, thus, still present.

91. *See Facebook liefert immer öfter Scheidungsgrund*, FRANKFURTER ALLGEMEINE ZEITUNG, Dec. 24, 2009, at 8.