Criminal Law Forum (2005) 16: 183–230
DOI 10.1007/s10609-005-4143-9

CLEMENS ARZT*

DATA PROTECTION VERSUS FOURTH AMENDMENT PRIVACY: A NEW APPROACH TOWARDS POLICE SEARCH AND SEIZURE

Enforcement of criminal law depends on information about facts and human beings as a major input. This piece is dealing only with the collection of information concerning human beings. Each human being at some moment has an interest in not letting the police, or the public, know what she or he is doing, with whom she or he communicates, where she or he meets with others, etc. On the other hand, police officers understand the collection of information to be a basic tool in the normal course of their business, limited if at all by constitutional provisions, or administrative rulemaking. Besides, collecting and using such information by the police is regulated in part by statute, for example, in the case of the interception of communications.[1] This article questions whether it is acceptable any longer to allow police to collect or use information on millions of citizens with very few clear-cut legal guidelines. The legal problem is whether Fourth Amendment[2] privacy ensures sufficient protection of civil liberties when it comes to police surveillance.

* Professor of Public Law, University of Applied Sciences in Administrative and Legal Affairs, Berlin/Germany (FHVR). Ass. iur., University of Bremen, 1988, Dr. iur., University of Bremen, 1989.

[1] See, *e.g.*, 18 U.S.C.A. §§ 2510–2522.

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

In 1890 Samuel Warren and Louis Brandeis, in an article for the *Harvard Law Review*, introduced the "right to privacy"[3] as a legal notion[4] in American law, then a mere civil law concept of a "right to be let alone".[5] Almost 30 years later one of the authors of this seminal article, now-Justice Brandeis, in his dissenting opinion in *Olmsteadt* v. *United States*[6], broadened the focus of the "tort privacy"[7] concept to be a right attributed to the citizens "against the Government" too. According to Brandeis, every "unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment".[8] It is probably not exaggerated to suggest that Justice Brandeis' dissent assisted at the birth of the very idea of Fourth Amendment privacy protection.[9] The Supreme Court another three decades later explicitly acknowledged in *Mapp* v. *Ohio*[10] that the "'security of one's privacy against arbitrary intrusion by the police' is 'implicit in "the concept of ordered liberty" and as such enforceable against the States through the Due Process Clause"'[11] of the Fourteenth Amendment. A few years later, while overruling *Olmsteadt*, the Court in *Katz*[12] laid the foundation for a modern understanding of Fourth Amendment protection.[13] In later cases[14]

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

[4] See Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1343–1357 (pointing out that there was no coherent notion of privacy in American law at this time).

[5] Warren & Brandeis, *supra* note 3, at 195 (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2nd ed. 1888)).

[6] 277 U.S. 438, 471 (1928), *overruled in Katz* v. *United States*, 389 U.S. 347 (1967).

[7] See Gormley, *supra* note 4, at 1340 (distinguishing five dominant species of legal privacy).

[8] *Olmstead*, at 478 (Brandeis, J., dissenting).

[9] The very notion of "privacies of life" was first used with reference to both, the Fourth and the Fifth Amendment in *Boyd* v. *United States*, 116 U.S. 616, 630 (1886).

[10] 367 U.S. 643 (1961).

[11] *Ibid.* at 650.

[12] *Katz*, 389 U.S. 347 (1967).

[13] "For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S. at 351–352 (citations omitted).

[14] See, *e.g.*, *California* v. *Ciraolo* 476 U.S. 207, 211 (1986); *Smith* v. *Maryland*, 442 U.S. 735, 740 (1979).

the Court referred to Justice Harlan's concurring opinion, evolving a two-fold test, according to which privacy protection requires "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'".[15] This approach is commonly referred to as the "reasonable expectation of privacy test".[16] The Supreme Court, while also using terms like "justifiable" or "legitimate" expectation of privacy, has consistently been applying this standard for more than three decades now.[17]

The problem with this ostensibly clear-cut standard is that hardly anybody is able to predict in a fairly reliable way if her or his behaviour or activity in a given situation will be deemed protected against police surveillance under Fourth Amendment privacy standards before the Supreme Court.[18] Even though the right to be let alone was labeled the "core content of privacy",[19] the Supreme Court never developed a comprehensive constitutional concept[20] of the very

[15] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[16] See, *e.g.*, 1 DAVID S. RUDSTEIN ET AL., CRIMINAL CONSTITUTIONAL LAW ¶ 2.03(2)(a) (2002).

[17] See, *e.g.*, *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001); *Bond* v. *United States*, 529 U.S. 334, 338 (2000) ("actual expectation of privacy"); *California* v. *Greenwood*, 486 U.S. 35, 41 (1988); *California* v. *Ciraolo*, 476 U.S. 207, 211 (1986); *Smith* v. *Maryland*, 442 U.S. 735, 740 (1979).

[18] See PHILLIPA STRUM, PRIVACY: THE DEBATE IN THE UNITED STATES SINCE 1945, 123 (1998) (speaking of a "tortuous path" the Court has taken since Katz in deciding whether law enforcement officers were acting unreasonably with regards to the fourth amendment) and Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757–758 (1994) (oversubtly summarizing "[W]arrants are not required – unless they are", *ibid.* at 757).

[19] David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. J. INT'L. L. 831, 831 (1991).

[20] See, *e.g.*, Flaherty, *supra* note 19, at 837 (concluding that Americans do not have an explicit federal constitutional right to privacy); Michael P. Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 SANTA CLARA COMPUTER & HIGH TECH. L. J. 71, 88 (1996); VINCENT J. SAMAR, THE RIGHT TO PRIVACY 51–82 (1991).

notion of privacy.[21] This might be attributed to the fact that legal privacy is a broad subject that might be broken down into various "classes". Aside from tort privacy, the subject may be split up into Fourth Amendment privacy, First Amendment privacy as a quasi-constitutional right between individuals, fundamental-decision privacy involving fundamental personal decisions protected by the Due Process Clause of the Fourteenth Amendment, and state constitutional privacy, resting upon state constitutional guaranties.[22] Other ways of splitting up privacy are certainly tenable.[23] Having this in mind, I will not dare to add another trial on the very notion of privacy.[24] Just as little will I add another piece on the widely held opinion that the Supreme Court does not effectively protect the right

[21] Cf. *Roe* v. *Wade*, 410 U.S. 113, 152 (referring to the fact that the Court or individual Justices have found the roots of privacy at least in the First, Fourth, Fifth, Ninth, and Fourteenth Amendment as well as in the penumbras of the Bill of Rights); *Paul* v. *Davis*, 424 U.S. 693, 712(1976) (even though there is no "right of privacy" in any specific guarantee of the Constitution, the Court has recognized "zones of privacy").

[22] Gormley, *supra* note 4, at 1340.

[23] See, *e.g.*, DARIEN A. MCWHIRTER & JON D. BIBLE, PRIVACY AS A CONSTITUTIONAL RIGHT 104 (1992) (distinguishing three major areas: rights to engage in sex, and marriage, to have an abortion, and freedom from searches that invade privacy); Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 744 (1989) (claiming that most privacy cases focus on sexuality in a broad sense); Samar, *supra* note 20, at 139–203 (adding some more subjects such as surrogate motherhood and the right to die); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 29–89 (1996) (adding voting rights and informational privacy); Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L. & COMP. L. REV. 661, 663–64 (1999) (differentiating (i) information privacy, concerning personal data, (ii) bodily privacy, concerning integrity of one's bodily integrity, (iii) communications privacy, and (iv) territorial privacy).

[24] See Gormley, *supra* note 4, at 1336 (stressing that hundreds of books and articles have been written on this subject). As of 25 July 2003 a search at LegalTrac© revealed 323 hits on "privacy AND Fourth Amendment" and 7773 hits on "privacy" alone.

to privacy rooted in the Fourth Amendment.[25] I shall rather try to elaborate on a different approach based on the idea of data protection in the context of police surveillance.

In this undertaking I will first try to throw light on the question why the very idea of data protection seems to be so unpopular with American scholars (I). After that the European Union's approach toward data protection, and the German concept of data protection in both, police and penal procedure law will be outlined (II). In a next step, some of the most seminal, and indeed controversial, Supreme Court's Fourth Amendment decisions related to police measures will be recalled. These cases will then be revisited from a data protection perspective. A very different outcome will be the result in most of these cases (III). Since data protection is a concept too different from Fourth Amendment privacy, I will propose a legislative approach to overcome the shortcomings of Fourth Amendment privacy when it comes to police surveillance (IV).

---

[25] See, *e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1974) ("For clarity and consistency, the law of the fourth amendment is not the Supreme Court's most successful product."); Jennifer Y. Buffaloe, *"Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule*, 32 HARV. C.R.-C.L. L. REV. 529, 530–531 (1997) (exceptions to warrant and probable cause requirements are numerous and the "special needs" rationale is making it easy to bypass both); Sherry F. Colb, *What is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of Remedy*, 55 STAN. L. REV. 119, 120–21 (2002) ("much of the universe of investigative activity does not even trigger the Fourth Amendment's reasonableness requirements"); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325 (2002); Sarah L. Shaeffer, Note, *Another Dent in our Fourth Amendment Rights: The Supreme Court's Precarious Extension of the Automobile Exception in Wyoming v. Houghton*, 45 S. D. L. REV. 422, 450 (2000) (the Court "deprives all persons traveling in vehicles the established protections of the Fourth Amendment"); Schwartz & Reidenberg, *supra* note 23, at 60–69 (judicial application of Fourth Amendment leaves it capable of protecting little more than the home and the curtilage). But see Stanley E. Adelman, *Safe at Home, But Better Buckle up on the Road – Supreme Court Search and Seizure Decisions, 2000–2001 Term*, 37 TUL. L. REV. 347 (2001) (Fourth Amendment rights came through said term in better shape than might have been expected). Some commentators emphasize *Kyllo* v. *United States*, 533 U.S. 27 (2001) in particular and indeed, this decision at least seems to reconfirm the strong protection of one's house when it comes to search and seizure.

I. DATA PROTECTION VERSUS PRIVACY

This piece is not about informational privacy in general. I shall rather question whether *reasonable expectation of privacy* as construed by the Supreme Court is a valuable concept to evaluate police surveillance and to protect people from unjustified governmental intrusion, which is the basic idea of the Constitution and the Bill of Rights.[26] Living in the "information age",[27] or in an "information society",[28] privacy issues and data protection are inseparably tied together. Nobody will seriously contest that government as well as many industries (*e.g.* credit card companies) today hold tremendous amounts of personal data in digitalized computer files for almost every living human being in the United States.[29] An increasing part of the general public seems to look upon this as a threat to privacy in the United States.[30] As early as 1977, the Supreme Court acknowledged a

[26] See Schwartz & Reidenberg, *supra* note 23, at 29 (the United States Constitution is the document through which the people establish their government and protect themselves from it).

[27] See, *e.g.*, FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997) (providing the notion of information age).

[28] See, *e.g.*, MICHAEL ROGERS RUBIN, PRIVATE RIGHTS, PUBLIC WRONGS: THE COMPUTER AND PERSONAL PRIVACY 59–73 (1988) (outlining the implications of living in an information society); Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L. J. 1321, 1326 (1992) (this term expresses the significance of the gathering, coordination, and analysis of data).

[29] See, *e.g.*, Schwartz, *supra* note 28, at 1329–1334 (modern service administration relies heavily on personal information); CATE, *supra* note 27, at 5–16 (with some basic information about the role of digitalized information in society today); STRUM, *supra* note 18, at 45–66 (on the privacy implications of the Social Security Number).

[30] See, *e.g.*, Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 752 (1999) (book review); PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 1–21 (1998).

possible privacy threat in the collection of personal information on the part of the Government.[31]

It seems to be indisputable that government's knowledge about citizens needs some limitations if Orwell's *1984* should not become true in the 21st century.[32] A good example of this is, perhaps, the control of libraries and bookstores in the post-9/11-era. In 2003, the Assistant Attorney General pointed out that the government does "not allow libraries or any other business to become safe havens for terrorist planning, financing, or communication".[33] This was meant to legitimize the control of business records in libraries and bookstores.[34] Not only the actual amount of information on every citizen but the mere possibility that government has vast amounts of personal data on citizens at its disposal may result *inter alia* in chilling effects on democratic activities, and on free speech. A society in which citizens do not know which governmental agencies might collect data about their life, their personal and political views, their social and private interactions, can no longer be considered a society based on the principle of liberty, because she or he may no longer feel free to

[31] "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Whalen* v. *Roe*, 429 U.S. 589, 605 (1977).

[32] See, *e.g.* Frank J. Eichenlaub, Note, *Carnivore: Taking a Bite Out of the Fourth Amendment*, 80 N.C. L. Rev. 315, 351 (2001) (Carnivore represents the nation's first journey into the use of the Internet as a law enforcement tool); Mark Elmore, Comment, *Big Brother Where Art Thou, Electronic Surveillance and the Internet: Carving Away From Fourth Amendment Protections*, 32 Tex. Tech. L. Rev. 1053, 1080 (2001) (privacy protection laws have failed to keep pace with the dangers of rapidly advancing technology); Schwartz, *supra* note 28, at 1387 (dangers of data processing exist in social administration programs; they may be even greater when used in the context of national security).

[33] Assistant Attorney General, Testimony before the Senate Committee on the Judiciary, 21.10. 2003: Protecting Our National Security from Terrorist Attacks: A Review of Criminal Terrorism Investigations and Prosecutions, *available at* http://judiciary.senate.gov/testimony.cfm?id=965&wit_id=2740. On the First Amendment implications see, *e.g.*, *Tattered Cover Bookstore*, *Inc.* v. *City of Thornton*, 44 P.3d 1044 (Colo. 2002).

[34] Cf. Dan Eggen, *Patriot Monitoring Claims Dismissed*, Wash. Post (Sept. 19, 2003) at A2 (after months of criticism from civil liberties groups and librarians the Attorney General felt inclined to stress that Section 215 of the USA Patriot Act, which allows authorities in terrorism investigations to obtain records from libraries and bookstores had never been used so far).

enjoy freedom of speech, or freedom of assembly, as the German Constitutional Court stated in its leading case on data protection.[35] This is especially true when it comes to police databases as most recently demonstrated by discussions about new counterterrorism databases.[36]

The capabilities of computers make it necessary to put some control on data gathering and data use by the government because computers have the ability to process and store vast quantities of information.[37] Processing such amounts of data was unimaginable in the pre-computer age.[38] Computer technology for this reason is continuously expanding the potential extent of surveillance. Certainly today, the bigger threat to the "ordinary" citizen in terms of daily annoyances rather stems from industry data collection and data use than from digitalized government files. Nevertheless, the accumulation of vast amounts of data on the part of the government is a threat to privacy as well.

The legal context in which "privacy" issues are addressed in the United States differs significantly from Europe[39] as well as from Germany.[40] A major difference certainly is due to the fact that legal regulation in the United States is based on pretty disparate sources, with federal, state, and local regulators sometimes following different concepts of how privacy may be protected against government

[35] German Federal Constitutional Court (Entscheidungen des Bundesverfassungsgerichts) [hereinafter BVerfGE] 65, 1, 43 (1983); see also Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084–1085 (2002).

[36] See, *e.g.*, Robert O'Harrow Jr., *U.S. Backs Florida's New Counterterrorism Database*, WASH. POST (Aug. 6, 2003) at A1. Editorial, *Spying by any name*, S.F. CHRON. (May 26, 2003) at A16.

[37] See, *e.g.*, Schwartz, *supra* note 28, at 1334–1343.

[38] SWIRE & LITAN, *supra* note 30, at 5–6.

[39] See SCHWARTZ & REIDENBERG, *supra* note 23, at 30–89 (discussing in depth the American concept of constitutional privacy protection as compared to the European Union's approach).

[40] These differences cannot be discussed here. For an analysis see, *e.g.*, Flaherty, *supra* note 19, at 841–843; Paul Schwartz, *The Computer in Germany and American Constitutional Law: Towards an American Right of Informational Self Determination*, 37 AM. J. COMP. L. 675, 686–692 (1989); SCHWARTZ & REIDENBERG, *supra* note 23, at 40–43.

actions. Some states have adopted explicit constitutional guarantees of privacy[41] that did not necessarily result in a higher level of privacy protection, however.[42] Many states introduced some kind of statutory protection[43] that may have some impact on data collection, data use, and information sharing, both within the government as well as between the government and private entities.[44] Absent substantial regulation, case law often results in little coherent guidance.[45] Different from Germany,[46] the Supreme Court has never made a finding on a right to the protection of personal data against police surveillance.[47] Even though the Supreme Court in an *obiter dictum* in *Whalen* v. *Roe* seemed to acknowledge a right of *informational privacy*,[48] the Court never further singled out this right in terms of a coherent means of protection against governmental, or police surveillance. Constitutional law hence provides no more than a ''kind of safety net'' for personal information or personal data waiting for completion by statutory law.[49] The Court seems to focus predominantly on the *protection of one's home*, which it sees '''at the very core' of the Fourth Amendment'' protection,[50] rather than on

[41] The California Constitution provides that ''[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, [. . .] and privacy.'' CAL. CONST. ART. I § 1. According to the Florida Constitution ''[e]very natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein''. FLA. CONST. art. I, § 23. See also CATE, *supra* note 27, at 66–68 (with reference to at least eight states that have privacy provisions in their constitution).

[42] CATE, *supra* note 27, at 68 (comparing *Hill* v. *Nat'l Collegiate Athletics*, 865 P.2d 633 (Cal. 1994) and *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995), both denying an unconstitutional encroachment in student's drug testing).

[43] See SCHWARTZ & REIDENBERG, *supra* note 23, at 129.

[44] *Ibid.* at 134–137 (with reference to California and Minnesota).

[45] CATE, *supra* note 27, at 49–50.

[46] The German Federal Constitutional Court in 1983 decided that every citizen is entitled to a right to informational self-determination (''Recht auf informationelle Selbstbestimmung''), deriving from the general right to the free development of one's personality (''allgemeines Persönlichkeitsrecht'') and the protection of the human dignity (''Menschenwürde''), as provided by art. 2 I and art. 1 I of the German Constitution (''Grundgesetz''), respectively. BVerfGE 65, 1/41–44.

[47] See *supra* note 20, and accompanying text.

[48] See *supra* note 31.

[49] SCHWARTZ & REIDENBERG, *supra* note 23, at 30–31.

[50] *Kyllo* v. *United States*, 533 U.S. 27, 31 (2001) (quoting *Silverman* v. *United States*, 365 U.S. 505, 511 (1961)).

informational privacy.[51] Above and beyond, the Supreme Court's construction of the Fourth Amendment does not leave it capable of protecting much more than men and women isolated in their homes or the immediate residential curtilage,[52] as the cases outlined in Section III demonstrate. Outside this very limited space, the Constitution as understood by the Supreme Court provides far less or even no protection at all. "Privacy" in the understanding of the Supreme Court thus does *not* "protect[s] the interest in keeping information out of the government's hands".[53]

Since constitutional law in the United States is rather designed to protect the most critical social and political values, much of protection is left open to the influence of the normal political process. One commentator pointed out more than a decade ago that privacy might not be an ideal normative concept for the computer age.[54] For this reason, data protection in the field of criminal procedure law can rather be expected from statutory law[55] than from the Fourth Amendment itself. This perspective is confirmed by quite a few pieces of federal legislation.[56] On a general level, the Privacy Act of 1974[57] has to be mentioned here since it seems to be the first recognition of a general interest in data processing and its potentially detrimental

[51] Sherry F. Colb, *The Qualitative Dimension of Fourth Amendment "Reasonableness"*, 98 COLUM L. REV. 1642, 1666 (1998) (concluding that the right to be let alone is a "concept that is distinct form the right to keep information secret from the government"); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L. J. 549, 583 (1990) (gathering of information is a new class of "intrusions" and fourth amendment protection has to be extended to protection of "informational privacy"). But see William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1021–1022 (1995) (claiming that "informational privacy" is preeminent in Fourth Amendment cases). However, Stuntz's claim seems to be rooted in his basic idea of focusing more on force and coercion and less on information gathering in criminal procedure law, see *ibid.* at 1060–1077.

[52] SCHWARTZ & REIDENBERG, *supra* note 23, at 60–61.

[53] Stuntz, *supra* note 51, at 1017 (1995).

[54] Schwartz, *supra* note 28, at 1347.

[55] SCHWARTZ & REIDENBERG, *supra* note 23, at 91.

[56] See Harold C. Relyea, *Personal Privacy Protection: The Legislative Response*, *in* PERSONAL PRIVACY 6–47 (Vita Cornelius ed., 2002) (furnishing a survey on privacy legislation). According to CATE, *supra* note 27, at 1, almost 1000 of 7945 bills introduced in the 104th Congress addressed some privacy issues.

[57] 88 Stat. 1896.

effects on the individual. In the field of police action some safeguards with regards to the interception of communications[58] were provided by the Omnibus Crime Control and Safe Streets Act of 1968,[59] the Electronic Communications Privacy Act of 1984 (ECPA),[60] and the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[61] The safeguards of these statutory provisions may well exceed those of the constitutional requirements.[62]

Yet, data protection in the United States still seems to be a rather exotic notion and many prefer to stick to privacy while data protection is the real subject.[63] The Supreme Court's precedents provide at most limited protection against government's intrusion upon one's (informational) privacy. Some protection exists where surveillance takes place at one's home. Constitutional provisions of some states and statutory law on the federal and state level provide some protection as well. Hitherto, it does not seem to be unjustified to sum up that neither federal constitutional law as construed by the Supreme Court nor statutory provisions have been able to provide sufficient legal protection for the individual affected by governmental collection and processing of personal data in general.[64] This seems to be equally true with regard to police surveillance.

---

[58] 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510–2522) [Interception of Wire, Electronic and Oral Communications].

[59] 82 Stat. 197.

[60] 100 Stat. 1848 (codified as amended at 18 U.S.C.A. §§ 2510–2522, 2701–2711 [Stored Wire and Electronic Communications and Transactional Record Access], and 3121–3127 [Pen Register and Trap and Trace Devices]. But see Tan, *supra* note 23, 671–672 (ECPA is vastly inadequate in terms of data protection).

[61] 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–1010) [Interception of Digital and other Communications].

[62] See, *e.g.*, *Brown* v. *Waddell*, 50 F.3d 285 at 290 (4th Cir. 1995).

[63] See, *e.g.*, SWIRE & LITAN, *supra* note 30, at 2 (explaining why their book refers to a "European Privacy Directive" which in its original terms is the "European Data Protection Directive"); SCHWARTZ & REIDENBERG, *supra* note 23 (calling their book "Data Privacy Law" to suggest the interdependence) and Samuelson, *supra* note 30, at 753 (1999) (book review) (assuming that even this title is too cryptic for an American audience). In an earlier piece Schwartz, *supra* note 28, at 1374–1386, is trying to develop the elements of an "American data protection law" for the administrative state while warning that grave dangers may arise when the state is using data processing to identify threats to national security (*ibid.* at 1387).

[64] See, *e.g.* Roch, *supra* note 20, at 93 (concluding that Congress has never consistently and coherently treated privacy concerns); Schwartz, *supra* note 28, at 1388 (data protection law is a medium to protect liberties of the individual).

II. BASIC PRINCIPLES OF DATA PROTECTION

Both the European Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data of 1995[65] and the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) of 1990[66] start from a very different point than the United States Supreme Court in its rulings on Fourth Amendment privacy. The Directive is not a statutory provision itself but obliges the member states of the European Union to enact statutory provisions in accordance with the rules laid out in the Directive. Nevertheless, Art. 3 of the Directive provides for the inapplicability of the Directive to security and criminal law because these fields are deemed to be outside of the legislative power of the European Union. German law does not exempt these areas from the general rules of data protection law but provides certain limitations on these general rules under well-defined conditions. German police law and German criminal procedure law thus both have incorporated data protection principles, although it is probably done more consistently in police law.

Both bodies of law provide for a catalogue of rights of every single person with regard to the collection, processing (*i.e.* storage, modification, transfer, blocking, and erasure[67]), and use of his or her personal data.[68] Personal data in this understanding is any information concerning the personal or material circumstances relating to an identified or identifiable individual, the so-called data subject. An identifiable person is one who can be identified, directly or indirectly,

---

[65] Council Directive 95/46 of 24 October 1995, 1995 O.J. (L281) [hereinafter Directive]. Legislation, official documents, and more information of the European Union can be found at http://europa.eu.int/index.htm. For a detailed discussion of the Directive see SWIRE & LITAN, *supra* note 30, at 22–151. This piece will not deal with the ongoing discussion whether transfer of personal data to the United States may violate the Directive; on this subject see, *e.g.*, Marsha Cope Huie *et al.*, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 92 TULSA J. COMP. & INT'L. L. 391 (2002).

[66] Federal Data Protection Act (*BDSG*) of 20 December 1990 (BGBl. I S. 2954) as amended [hereinafter *BDSG*]. An English translation as of January 1, 2003 is provided, *e.g.*, at www.bfd.bund.de/information/bdsg_eng.pdf. A still valuable introduction to the general concept of data protection law in Germany gives J. Lee Riccardi, Note, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy*, 6 B.C. INT'L. & COMP. L. REV. 243 (1983).

[67] *§3(4) BDSG*.

[68] *§3 BDSG*.

in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.[69] Both German and European data protection law do not draw any line between "sensible" personal data that does need protection and less sensible ones, thus avoiding any problems in definition and distinction.[70] Data protection therefore embraces the control of all kinds of personal data relating to an individual. Not only information like name, age, sex, or religion are personal data. Information on the content of communications as well as information about a person's whereabouts is personal data as well. This is not dependent on whether the person is in public or within his or her home, or curtilage. For this reason, what a person "knowingly exposes to the public"[71] can still be personal data as long as it is information concerning the personal or material circumstances of an identified or identifiable individual. Accordingly, taking part in a political demonstration, talking in public to somebody, driving from A to B, or walking from my house to a library is information concerning my personal habits, or interest, or beliefs. Police surveillance of such activities constitutes collection of personal data.

In Europe, the German Federal Data Protection Act is probably one of the most stringent data protection statutes, due to experiences with data collection, and surveillance by police and secret services during the Nazi era.[72] In 1983, the German Federal Constitutional Court (*Bundesverfassungsgericht*) decided that data protection is a constitutional principle and thus requires specific statutory rules for any kind of data collection and processing before such data collection, processing, or use takes place.[73] Consistent with this "overall" data protection approach, German police law[74] does not even need to give a definition of personal data but only implicitly refers to such definition in § 3(1) of the German Federal Data Protection Act, or state data protection law, respectively. The police may not collect or

---

[69] Directive at art. 2(a) and § 3(1) BDSG.

[70] See Riccardi, *supra* note 66, at 249, and Directive at art. 2(a): "any information relating to an identified or identifiable natural person".

[71] *Katz* v. *United States*, 389 U.S. 347, 351 (1967).

[72] See Huie *et al.*, *supra* note 65, at 393 n.4 (Germany and France have been the sternest protectors of the right to personal privacy in the western world after WWII).

[73] *Supra* note 46.

[74] Different from the United States, Germany has a clear and distinct separation of police law that is under the legislative sovereignty of the 16 States (*Länder*) on the one hand while criminal procedure law on the other hand is under the legislative sovereignty of the federal parliament (*Bundestag*).

process any personal data as long as they are not specifically, and explicitly, authorized to do so under statutory law. State[75] police law,[76] as well as the Federal Criminal Procedure Code,[77] provide for data collection and data processing since the 1980s, with many regulations in the Federal Criminal Procedure Code of a much younger age, however.[78] Thus, under German police law data collection is admissible, *e.g.* if this is necessary to prevent a crime, but only if there are grounds that such crime might occur in a given case. In case of imminent danger, identification might be an appropriate means of collecting personal data. Any kind of (open or covert) surveillance of a person is regarded to be data collection and thus needs statutory justification and must adhere to statutory law, too. Video surveillance in public places, and automatic number plate reading, are being discussed for a couple of years now. Some German States did introduce legislation on these means of data collection while others have chosen not to do so because legislators think this covers too many people who neither constitute a danger to public safety nor are suspected of having committed a crime. In general, covert data collection is regarded as being far more intrusive than open action by the police. For this reason covert action regularly requires a "shift" in decision making; *i.e.* only a high ranking senior officer might be allowed to decide on the use of such means, or even prior judicial control is required by the relevant statute. In cases of covert data collection the "data subject", *i.e.* the person under surveillance, has a constitutional right to be informed about such activities by the police once the reason for surveillance ceases to exist. The Federal Criminal Procedure Code also provides for comparable means of data collection where a criminal offense has taken place.

Even though I will apply the very idea of data protection in some of the Supreme Court's leading cases on police surveillance, I am not going to undertake an analysis of every single case according to German, or European data protection, police, or criminal procedure

[75] Statutory power in police law rests with the parliaments of the 16 German States while statory power in criminal procedure law rests with the Federal Legislator.

[76] See, *e.g.*, § 19 Police Code of Baden-Württemberg (*Polizeigesetz für Baden-Württemberg*); §§ 9, 15 Police Code of North-Rhine Westphalia (*Polizeigesetz Nordrhein-Westfalen*); § 18 Code of Public Security and Order Berlin (*Allgemeines Sicherheits- und Ordnungsgesetz Berlin*).

[77] *Strafprozessordnung* (hereinafter *StPO*), first enacted in 1877.

[78] See, *e.g.*, §§ 98a, 98d 163d, 483, 484 *StPO*.

law, due to the many differences in the legal regimes of these entities. What I will focus on is the substitution of the American privacy concept with the concept of data protection when it comes to search and seizure, and other means of police surveillance. What I am trying to bring out in this piece is that the very idea of legally protected personal data would lead to a very different outcome in many Supreme Court privacy cases. Protection of personal data is deemed to result in a more predictable approach towards what kind of human activities, movements, behavior, communications, and personal records does the law protect and under which prerequisites police (only) may collect such data. Applying a data protection approach would hence probably result in a better protection of privacy or, better, liberty of the person under surveillance.

III. FOURTH AMENDMENT PRIVACY REVISITED

As noted earlier, this is not the place to discuss for the umpteenth time leading Fourth Amendment cases of the Supreme Court and to complain about the Court's failure to protect privacy. Instead, I will outline some of the perhaps most typical and important police surveillance cases since *Katz*.[79] The selection of cases certainly is not conclusive and other classes of search and seizure do exist. To a certain extent, the selection is biased to be able to demonstrate in which field a data protection approach might be more appropriate than the Supreme Court's approach toward Fourth Amendment privacy protection. One might consider the selection "biased" in as much as I decided to take a close look at such subjects that seem to be most troubling from a perspective of data protection. I did not look at such classes of search and seizure that are highly controversial because of the technologies involved, for example cellular phone tracking, email, and Internet use and its possible implications on Fourth Amendment protection, because no Supreme Court decisions on these subjects are available yet. One might regret that. On the other hand, as the recent decision in *Kyllo*[80] shows, the Court may not be immune to the threats of modern technologies in terms of privacy protection. Speculation about the outcomes of future cases should not be the business of a foreign lawyer, though.

---

[79] 389 U.S. 347 (1967).

[80] *Kyllo* v. *United States*, 533 U.S. 27 (2001).

In this section, I will present major Supreme Court cases on Fourth Amendment privacy. These cases shall only be introduced as far as the underlying question of the data protection versus the privacy concept is concerned. Fourth Amendment cases not primarily dealing with privacy issues will not be dealt with here. This applies, for example, to arrest or bodily searches respectively. After the presentation of the cases, I will briefly re-examine these decisions. A good starting point in many cases is the dissenting opinions, in some others the concurring ones already give an idea of a possible different approach. However, the focus here will be on a re-examination from a data protection perspective. What I will try to show is that in most of these cases, which are very typical, a data protection approach would lead to a different outcome when it comes to privacy questions.

3.1. *Plain View and Open View*

In *Coolidge* v. *New Hampshire*,[81] the Court had to decide whether evidence gathered in a car could be used as evidence against the suspect despite being a warrantless[82] search. According to the Court, "it is well established that under certain circumstances the police may seize evidence in plain view without a warrant".[83] At the same moment, the Court notes, however, that virtually "any evidence seized by the police will be in plain view, at least at the moment of seizure".[84] The Court further stressed that plain view may legitimize a seizure if the "police have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character".[85] Seizure is permissible also where an object comes into plain view during the course of action that is supported by one of the "recognized exceptions to the warrant requirement",[86] as is the case with hot pursuit of a fleeing suspect, for example. The Court summarized that plain view is given only in so far as the police officer "had a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence" that is later being used against the accused.[87] Whereas in *Coolidge* the

[81] 403 U.S. 443 (1971).
[82] The warrant was held to be invalid, *ibid.* at 449.
[83] *Ibid.* at 465.
[84] *Ibid.*
[85] *Ibid.*
[86] *Ibid.*
[87] *Ibid.* at 466.

Court held that the discovery of the seized object in plain view must be "inadvertent",[88] this requirement was later abandoned in *Horton* v. *California*.[89]

In case plain view is invoked, probable cause is required in order to legitimize a seizure.[90] Plain view provides a legal basis for a warrantless seizure,[91] even though the seized objects were not legitimate objectives of that search. Yet, this does not mean that no search has taken place.[92] Plain view requires prior justification for the entry in one's home or some other justification like a search incident to arrest.[93]

There are some cases in general labeled as plain view, even though no prior Fourth Amendment intrusion has taken place. Professor LaFave and others propose a different term for these cases to avoid confusion with the principles outlined above. Open view, plain sight, and other notions have been proposed.[94] Open view refers to a situation in which an observation is made by a police officer without prior physical[95] intrusion into a constitutionally protected area. These situations encompass discovery outside a constitutionally protected area like open fields, which will be dealt with later.[96] Also mentioned are cases like police officers observing an individual, object, or activity in any place open to the public, provided any member of the public could have made the observation.[97]

---

[88] *Ibid.* at 469.

[89] *Horton* v. *California*, 496 U.S. 128, 138–140 (1990).

[90] *Arizona* v. *Hicks*, 480 U.S. 321, 326 (1987).

[91] Howard E. Wallin, *Plain View Revisited*, 22 PACE L. REV. 307, 325 (2002) (plain view refers only to seizure but not to search).

[92] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE §§ 2.1–2.7 (3rd. ed. & Pocket Part 2003) § 2.2(a).

[93] Wallin, *supra* note 91, at 324.

[94] See LAFAVE, *supra* note 92, § 2.2(a); Wallin, *supra* note 91, at 324–325. Both, LaFave and Wallin refer to Charles E. Moylan, *The Plain View Doctrine: Unexpected Child of the Great "Search Independent" Geography Battle*, 26 MERCER L. REV. 1047, 1096–1101 (1975) (distinguishing open and plain view). See also *Texas* v. *Brown*, 460 U.S. 730, 738 n.4 (1983) (plain view, as used in *Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971), to justify seizure of an object has to be distinguished from an officer's "mere observation of an item left in plain view").

[95] However, a particularly intrusive method of viewing (only) may be an intrusion upon a constitutionally protected expectation of privacy; see RUDSTEIN *et al.*, *supra* note 16, ¶ 2.03(2)(c)(ii)(A) and notes 191–193.

[96] See *infra*.

[97] RUDSTEIN ET AL., *supra* note 16, ¶ 2.03(2)(c)(i) (quoting dozens of cases from various jurisdictions).

Accordingly, the Supreme Court does not regard monitoring the movements of a person in public places and streets to be a search.[98] This is equally true in cases where a police officer observes an object on the person of an individual, inside the dwelling[99] of somebody or on the exterior of a car.[100] The interior of an automobile "which may be viewed from outside the vehicle by either inquisitive passerby or diligent police officers"[101] as well is not protected under the Fourth Amendment against observation by police and such observation does not constitute a search, due to the lack of a reasonable expectation of privacy. While the Supreme Court never has referred to "open view" for such cases, other courts have done so.[102]

Opening the door of a car, sticking the head inside the vehicle, or entering the vehicle itself may constitute a search within the meaning of the Fourth Amendment.[103] Nevertheless, no encroachment upon constitutionally protected rights occurs as long as such observation can be made without any intrusion into the observed area itself, since the Fourth Amendment does not require police officers to "shield their eyes when passing by a home on public thoroughfares".[104] What the police may see from a "public vantage point" thus is not protected from inspection as far as they have a "right to be" there.[105] Lacking prior intrusion, no prior justification is necessary either, as

[98] "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *United States* v. *Knotts*, 460 U.S. 276, 281 (1983).

[99] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz* v. *United States*, 389 U.S. 347, 351 (1967).

[100] "The exterior of a car . . . is thrust into public eye, and thus to examine it does not constitute a 'search'". *New York* v. *Class*, 475 U.S. 106, 114 (1986). This may well imply the examination of the tire on the wheel and taking of paint scrapings from the exterior of a car left in a public parking lot. *Cardwell* v. *Lewis*, 417 U.S. 583, 591 (1974).

[101] *Texas* v. *Brown*, 460 U.S. 730, 740 (1983).

[102] See, *e.g.*, *State* v. *Clark*, 859 P.2d 344, 349 (Idaho App. 1993) (open view refers to situation where law enforcement officer observes incriminating evidence from non-intrusive vantage point); *Brown* v. *State*, 292 A.2d 762, 778 (1972) (open view furnished ample probable cause to believe that items were contraband); Wallin, *supra* note 91, at 324–345 (with an in depth analysis of various court rulings on plain view and open view, respectively).

[103] RUDSTEIN ET AL., *supra* note 16, ¶ 2.03(2)(c)(ii)(C) and notes 269–275; *New York* v. *Class*, 475 U.S. at 114–15.

[104] *California* v. *Ciraolo*, 476 U.S. 207, 213 (1986).

[105] *Florida* v. *Riley*, 488 U.S. 445, 449 (1989).

long as no further action is taken.[106] Nonetheless, even though the police have a legitimate right to observe an item they consider to be evidence of a crime this does not justify a warrantless intrusion into a constitutionally protected area.[107]

3.2. *Plain View and Open View Revisited*

In the following section I will thoroughly work through the topics of plain view, and open view as an example which demonstrates the differences between the data protection approach and the Supreme Court's privacy approach.

3.2.1. *Search or Seizure*

In *Texas* v. *Brown*,[108] the Court stated that "plain view" might denote two very different situations that need to be distinguished. While the "mere observation of an item left in plain view"[109] does not involve a Fourth Amendment search, the seizure of such an object in general does implicate the Fourth Amendment's limitations upon the seizure of personal property.[110] Quoting *Payton* v. *New York*[111] the Court further emphasized that the seizure of an object found in a public place involves no invasion of privacy and is presumptively reasonable where there is probable cause to associate such property with criminal activity.

From a data protection perspective a clear distinction between search and seizure must be made. The *seizure* of a tangible item does not *itself* imply the collection of data. Data collection may only result from such seizure, in case the seized item contains or reveals personal data that is being 'extracted' by the police. Thus, we only have to take a closer look at data collection by means of observation of an item or of a natural person[112] in plain view or plain sight. Even a (short) observation of a car and a check of the license plate reveal data on the owner and the use of his car. For this reason, such a simple check, which is day-to-day routine of police officers, has to be considered data collection.

---

[106] LaFave, *supra* note 92, § 2.2(a).

[107] Wallin, *supra* note 91, at 325; RUDSTEIN ET AL., *supra* note 16, ¶ 2.03(2)(c). Moylan, *supra* note 94, at 1096 (emphasizing, "wherever the eye may go, the body of the policeman may not necessarily follow").

[108] 460 U.S. 730 (1983).

[109] *Ibid.* at 738 n.4.

[110] *Ibid.*

[111] 445 U.S. 573, 587 (1980).

[112] Only natural persons are entitled to data protection, according to Directive art. 2(a) and § 3(1) *BDSG*.

3.2.2. *Information Gathering – Is there any Difference between the Police and the General Public?*

In the case underlying the decision in *Texas* v. *Brown*,[113] Brown's car was stopped at a routine driver's license checkpoint. The police officer asked Brown for his driver's license and then changed his position and bent down at an angle to see what was inside Brown's car.[114] Since the general public could have peered into the interior of said car as well,[115] the Court denied any legitimate expectation of privacy on the part of Brown who was carrying a balloon containing drugs. The Court concluded that the conduct that enabled the police officer to observe the interior of the car was not a search within the meaning of the Fourth Amendment.[116]

The case is a good example how Fourth Amendment protection under the reasonable expectation doctrine ties protection against police surveillance to what the common citizens expect from one another, not what they expect from the police.[117] For this reason the assumption that the Constitution does not exclude the police from observing what every member of the public can see[118] is sound under Fourth Amendment standards. Conversely, it is not compatible with the protection of personal data. The problem is not to require the police to look away when everyone else may observe.[119] Nevertheless, to treat police and "ordinary" citizens the same does not take into account the undisputable fact that the general public is distinct from the police and *vice versa* with regard to the collection of personal data.[120] The general public as well as the police may gather

[113] 460 U.S. 730 (1983).

[114] *Ibid.* at 733.

[115] *Ibid.* at 740.

[116] *Ibid.*

[117] William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1268 (1999) (tying Fourth Amendment protection to what people expect from the government would be useless because the government could easily influence these expectations).

[118] *California* v. *Ciraolo*, 476 U.S. 207, 224 (1986) (Powell, J., dissenting).

[119] Nevertheless, this seems to be the common understanding of the concept of knowing exposure, see, *e.g.*, Colb, *supra* note 25, at 124 ("The police need not avoid looking at what everyone else can see.").

[120] See Ku, *supra* note 25, at 1371 ("the fact that citizens may invade each other's privacy does little to answer the question of whether the government should have the same power"); Amsterdam, supra note 25, at 406 (voluntary assumption of risk of betrayal in ordinary social intercourse does not mean that government is constitutionally unconstrained in adding to those risks).

information, for example, about the movements of a certain person in the public, whom she or he is meeting, with whom she or he is associated while attending a demonstration, when she or he visits the offices of a drug treatment center and so forth. From the Supreme Court's point of view, this results in a no search verdict.

In contrast to this approach, one commentator recently proposed to define a search or seizure as an exploration, searching out, or process by which the police look for information. The threshold would be whether the police were "looking for specific information or data" or if they were "targeting a specific location, person, or object".[121] What makes the difference? First, the government has vast resources of data collection and data storing at its disposal and may use such data for future law enforcement against the observed person.[122] Second, the police have the constitutional power to deprive the person under surveillance of his or her freedom. Third, the Bill of Rights limits the action of police, not private action.[123] These factors clearly distinguish the government substantially from every private actor and therefore the government and its agents cannot be treated like a citizen when it comes to data protection.

3.2.3. *Texas v. Brown*

Turning back to *Texas* v. *Brown*, the approach just outlined above would lead to a different perspective. Brown withdrew his hand from his pocket and he held a green party balloon between his fingers.[124] The police officer then "shifted his position in order to obtain a better

[121] Gregory S. Fisher, *Cracking Down on Soccer Moms and Other Urban Legends on the Frontier of the Fourth Amendment: Is It Finally Time to Define Searches and Seizures?*, 38 WILLAMETTE L. REV. 137, 172 (2002). While Fisher refers to the "objective manifestations of police conduct" a data protection approach rather refers to the purpose of police action. This does not mean, however, to scrutinize "subjective intent" or "motive", see *Whren* v. *United States*, 517 U.S. 806, 813–814 (1996), but refers to the objective purpose of a specific conduct or measure.

[122] See George M. Derry III, *The Loss of Privacy Is Just A Heartbeat Away: An Exploration of Government Heartbeat Detection Technology and Its Impact on Fourth Amendment Protections*, 7 WM. & MARY BILL RTS. J. 401, 440 (1999) (inspection of an individual by a corporation is different from governmental intrusion because the government possesses the resources to prosecute and punish).

[123] Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 429 (1997); see also *Burdeau* v. *McDonell*, 256 U.S. 465, 475 (1921) (Fourth Amendment protection is "not intended to be a limitation upon other than governmental agencies").

[124] *Texas* v. *Brown*, 460 U.S. at 733.

view'' and subsequently noticed several items in the glove compartment that he attributed to the use of illicit drugs.[125] This makes clear that we are not looking at a very short, spontaneous or otherwise inevitable observation on part of said police officer. Even the very first observation had nothing to do with the purpose of the police checkpoint which was supposed to be a ''driver's license checkpoint''. The police officer did not inadvertently observe Browns movements and action, but ''at roughly the same time'', after having asked for the driver's license, he intentionally ''shined his flashlight into the car''.[126] This was not an unavoidable and inadvertent component of the driver's license check. It rather constituted a common police practice to check and actually search[127] at least the passenger compartment as far as possible by peering into each car that has been stopped.[128] For these reasons, it is without doubt that the police officer was intentionally trying to collect information[129] about the person being stopped at the routine checkpoint. This was information about an identifiable person at a given place and a given time. In consequence, a collection of personal data took place.

3.2.4. *Knotts*

In *Knotts*,[130] the Court held that people traveling in an automobile on public thoroughfares have no reasonable expectation of privacy. Such persons ''voluntarily conveye[d] to anyone who wants to look the fact that he [or she] was traveling over particular roads in a particular direction, the fact of whatever stops'' he or she made as well as information about his or her final direction.[131] The Court

[125] *Ibid.* at 734.

[126] *Ibid.* at 733.

[127] See Amsterdam, *supra* note 25, 396 (when a police officer shines his or her flashlight into a parked car he or she is carrying out a search if one looks at it from the plain meaning of the English language).

[128] Powell, J., concurring, *ibid.* at 746, asserts that the police officer's action was a ''lawful inspection of the front seat area'' without further elucidating the necessity or reason for such an inspection.

[129] See Stuntz, *supra* note 51, at 1023 (if the law seeks to protect ''informational privacy'', each marginal search, each additional place where the officer casts his or her eye, requires justification).

[130] *United States* v. *Knotts*, 460 U.S. 276 (1983).

[131] *Ibid.* at 281–282.

equaled the use of a beeper to "[v]isual surveillance from public places" and consequently the use of a beeper does not alter the situation, according to the Court.[132] While relying on an army of "hypothetical bystanders"[133] the Court again misses the important distinction that "anyone" is not the police and vice versa. Looking at this case from a data protection perspective shows that the movements of a person on public thoroughfares and his or her destination are personal data *par excellence*.

The decision does not clearly state whether Petchen, the person whose movement by car was observed by use of a beeper, was already an identified individual at the time of observation. However, Petchen was identifiable at least; otherwise, he would not have been charged in court. Observing his movements on public streets and his final destination in a private cabin the police were acquiring information relating to an individual for the purposes of criminal investigations. This information *inter alia* referred to his whereabouts during the time of driving, the fact and the time of driving itself, the fact that he passed this and that area, street, town, and so on. Moreover, the place, or person respectively he was heading to, when he arrived at Knott's cabin, were identifiable. Thus, information about whom he was visiting was equally collected. Petchen obviously was the (data) subject of an ongoing criminal investigation. In addition, when Petchen was driving off the road and heading into Knotts' private premises, the police were collecting personal data about a different person (Knotts) also.

While acknowledging Knotts' reasonable expectation of privacy within his cabin, the Court refused to accept any privacy expectations with regard to the visual observation of Petchen's automobile arriving at Knotts' premises, and to the movement of objects outside the cabin in the open fields.[134] This again would be judged differently under a data protection perspective. Collecting data about who is going to visit an identified or identifiable person is collection of personal data since it reveals information about privately, socially or otherwise initiated human contacts or relations. This is true when it comes to Knotts' movement of objects outside his cabin. Here the police were collecting information on behavioural facts or activities of this data subject. Especially with regard to the "drum of chloroform outside the cabin",[135] the police obviously did not inadvertently

[132] *Ibid.* at 282.

[133] LaFave, *supra* note 92, § 2.7(e).

[134] 460 U.S. at 282.

[135] *Ibid.*

observe innocent movements of, *e.g.*, a butterfly, or a child[136] on the premises. Instead, they observed purposely the movement of an object that was supposed to be an important item of evidence in an ongoing criminal investigation. For this reason, it is without doubt that this was a collection of data and Knotts was the data subject.

3.2.5. *Cardwell v. Lewis*

In *Cardwell* v. *Lewis*,[137] the taking of paint scrapings from the exterior of the suspect's car itself may not be seen as collection of personal data. Nevertheless, this action was aimed at gaining information about the possible involvement in an accident or other "physical contact" with another car. It was clear from the very beginning that the information was supposed to be used in a criminal investigation. In fact, the comparison of the paint scrapings taken from the victim's car with the paint from the suspect's car lead the police to detect at least a physical contact of both cars, thus revealing information about the suspect's probable involvement in the crime. The Court's statement that if a search took place at all, the invasion of privacy was "abstract and theoretical"[138] conflicts with the fact that the police took a sample from the suspect's car with the very purpose to collect evidence in an ongoing criminal investigation. Thus, data collection took place here, too.

3.2.6. *New York v. Class*

In *New York* v. *Class*,[139] a data protection approach would probably not lead to a result different from the Court's decision. It must be taken into consideration that the Vehicle Identification Number (VIN) itself does not contain personal data.[140] On the other hand, attributing a certain car to a given person constitutes collection of personal information about a (natural) person. The statement, a car with VIN *#XYZ* belongs to Mister or Misses so-and-so, certainly provides personal information about said person. In *Class*,

[136] While a short glance may not constitute the collection of personal data this is no longer true when a police officer begins to *observe* somebody or something that may be attributed to an identified or identifiable person.

[137] 417 U.S. 583 (1974).

[138] *Ibid.* at 592.

[139] 475 U.S. 106 (1986).

[140] See 49 CFR § 565 (2002).

conversely, it was not this kind of information but the gun that was sought to be suppressed in evidence.[141] Therefore, a data protection approach would not lead to a different result.

3.3. *Open Fields and Curtilage*

The open field doctrine goes back to the Supreme Court decision in *Hester* v. *United States* in 1924 when the Court held that Fourth Amendment protection of persons, houses, papers, and effects does not extend to "open fields".[142] Open fields may encompass any "unoccupied or undeveloped area outside of the curtilage" which neither needs to be "open" nor a "field".[143] A police officer may set foot on an open field without either probable cause or reasonable suspicion.[144] However, if a constitutionally protected building or area is 'surrounded' by an open field, the open field may still be entered but, for example, not a barn in the middle of such an open field.[145]

In *Maine* v. *Thornton*,[146] the case consolidated with *Oliver* v. *United States*,[147] the police officers, while checking an anonymous tip, entered the woods by a path between Thornton's residence and a neighboring house. They discovered two marijuana fields that they later determined to be on Thornton's property.[148] The Court held that nobody may "legitimately demand privacy for activities out of doors in fields, except in the area immediately surrounding the home".[149] Again, the Court relied on the fact that the relevant lands were equally accessible to the public and the police.[150]

---

[141] 475 U.S. at 114.

[142] 265 U.S. 57, 59 (1924).

[143] *Oliver* v. *United States*, 466 U.S. 170, 180 n.11 (1984).

[144] *United States* v. *Dunn*, 480 U.S. 294, 304 (1987) (police officers legally entered a field protected by several fences); see also *Oliver*, 466 U.S. at 179 (surveillance of open fields is no privacy intrusion because there is no societal interest in the protection of privacy in open fields).

[145] *Dunn*, 480 U.S. at 304.

[146] 466 U.S. 170 (1984).

[147] 466 U.S. 170 (1984).

[148] *Ibid.* at 174.

[149] *Ibid.* at 178.

[150] *Ibid.* at 179.

On various occasions, the Court emphasized that the sanctity of the private[151] home is at the centre of Fourth Amendment protection.[152] The constitutional protection of the home includes the curtilage, which makes it necessary to distinguish the protected space (curtilage) from the unprotected area outside. According to the Court, the common law provided for a clear distinction under which the curtilage was the land ''immediately surrounding and associated with the home'' and dedicated to the ''intimate activity associated with the sanctity of a man's home and the privacies of life''.[153] As it is true for the house, the protection of the curtilage is aimed at the protection of families and personal privacy. It is limited to an ''area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened''.[154] To distinguish open fields from curtilage the Supreme Court developed a four-fold test, one that is not supposed to be applied in a mechanical way however.[155] Accordingly, limitations on privacy occur where curtilage protection is denied to a particular space or where a reasonable expectation of privacy is denied.

Under German law, an area deemed one's home[156] is provided a separate and very high level of constitutional protection under art. 13(1) of the Federal Constitution (*Grundgesetz*).[157] Encroachments upon the constitutional guarantees of the home are not judged by

[151] According to *Dow Chemical Co*. v. *U.S*., 476 U.S. 227, 234–239 (1986), commercial premises do not enjoy the same level of protection like private homes.

[152] See, *e.g*., *Wilson* v. *Layne*, 526 U.S. 603, 610–611 (1999); *Payton* v. *New York*, 445 U.S. 573, 585, 601 (1980).

[153] *Oliver*, 466 U.S. at 180 (citations and quotation marks omitted).

[154] *California* v. *Ciraolo*, 476 U.S. 207, 212–213 (1986).

[155] ''[C]urtilage questions should be resolved with particular reference to four factors: the proximity of the area claimed to be curtilage to the home, whether the area is included within an enclosure surrounding the home, the nature of the uses to which the area is put, and the steps taken by the resident to protect the area from observation by people passing by. . . . [W]hether the area in question is so intimately tied to the home itself that it should be placed under the home's 'umbrella'(...) of Fourth Amendment protection.'' *Dunn*, 480 U.S. at 301.

[156] This may include the close surroundings of said home, *e.g*., the backyard. Nevertheless, as is the case in the United States, there might be some argument about constitutional protection for a particular space. This is not a problem of data protection, however.

[157] ''The home is inviolable.''

data protection standards but by said constitutional provision, which protects the home as a last retreat of personal privacy, and human dignity.[158]

In *Oliver* v. *United States* as well as in *Maine* v. *Thornton*,[159] the police undertook some effort to arrive at the space they planned to inspect. Obviously, the police officers did not inadvertently happen to discover the marijuana patches but this was the result of a purposeful undertaking. The police discovered the marijuana patches after having received reports or tips on such activities. Accordingly, the police were looking for such information that might help convict the suspected person. Thus, the police were collecting data on an identified (Oliver), or identifiable (Thornton) person, respectively.

3.4. *Aerial Surveillance*

For 25 years now aerial surveillance has become a frequently used surveillance technique in day-to-day police operations. While some law enforcement agencies conduct routine surveillance flights to look for possible violations of the law, it seems to be more common to use aircrafts or helicopters in case some information exists that criminal activity is afoot on a certain property but police lack probable cause to obtain a search warrant.[160]

The Supreme Court took a close look at the constitutional question whether such means of surveillance have to be judged by Fourth Amendment standards or not in three decisions in the mid 1980s. In 1986, the Court had to give an opinion on two different surveillance techniques. In the case of *California* v. *Ciraolo*,[161] the police received an anonymous telephone tip that marijuana was grown in someone's backyard. Due to two different fences completely enclosing the yard, the police officers were unable to observe this yard from ground level. Using a private airplane, they flew over the house at an altitude of 1000 feet and identified the incriminating plants.[162] Since the Court deemed the yard to belong to the curtilage the constitutional question

[158] BVerfG NJW 2004, 999 (*"absolut geschützter Kernbereich privater Lebensgestaltung"*).

[159] 466 U.S. 170 (1984).

[160] RUDSTEIN ET AL., *supra* note 16, ¶ 2.03(2)(g) and n.316–317 (with reference to various court decisions).

[161] 476 U.S. 207 (1986).

[162] *Ibid.* at 209.

was whether "naked-eye observation" from an airplane violates a reasonable expectation of privacy. With reference to the decisions in *Knotts*[163] and *Katz*[164] the Court declared that the police are neither obliged to shield their eyes when passing a home on public thoroughfares nor could restrictions of some views of someone's activities preclude observations from a public vantage point where the police have a right to be.[165] Because any member of the public could have seen what the police observed by simple naked eye from aboard the airplane no reasonable expectation of privacy in the activities in the curtilage existed according to this ruling[166] and the Court denied that a search had taken place.

The same day, the Court in *Dow Chemical* v. *United States*[167] also upheld the constitutional permissibility of airborne observations by means of a commercial aerial mapping camera. In this case, it was not a private home or curtilage being observed but an industrial plant, which the Court deemed to be more comparable to an open field.[168] While the company conceded that naked-eye observations of said plant would not have amounted to a search,[169] the question was whether the use of sense enhancement equipment was of any influence on the constitutional questions. Even though the use of said camera gave "more detailed information than naked-eye views", it was not able to "penetrate the walls". The information was "limited to an outline" of the company's facilities. Enhancing the human vision "somewhat, at least to the degree here", does not amount to a search according to the Court.[170] For these reasons, the Court held that no search had taken place here, either.

Three years later a case very similar to *Ciraolo* was decided. In *Riley*[171] the police received an anonymous tip about marijuana being grown on somebody's private property. The property was fenced, and a "Do Not Enter" sign was posted. For these reasons, the police were not able to observe the contents of a greenhouse on the property from the road. The police circled twice over the property in a helicopter at

[163] *United States* v. *Knotts*, 460 U.S. 276, 282 (1983).
[164] *Katz* v. *United States*, 389 U.S. 347, 351 (1967).
[165] *Ciraolo*, 476 U.S. at 213.
[166] *Ibid.* at 213–215.
[167] 476 U.S. 227 (1986).
[168] *Ibid.* at 239.
[169] *Ibid.* at 234.
[170] *Ibid.* at 238.
[171] *Florida* v. *Riley*, 488 U.S. 445, 448 (1989).

the height of 400 feet making naked-eye observations through the greenhouse roof.[172] The Court[173] considered the use of helicopters in private and commercial life a routine in today's world.[174] Consequently, any member of the public could have made the same observations as the police did. The Court therefore denied a reasonable expectation of privacy. This could have been judged differently only "if flying at that altitude had been contrary to law or regulation", the Court stated.[175] An encroachment seems to be possible also in case the applied means interfere with the "normal use" of one's home or curtilage. This is, *inter alia*, the case if "undue noise", "wind, dust, or threat of injury" occur.[176] In *Riley*, the Court also revealed that no "intimate details connected with the use of the home or curtilage were observed"[177] without further explaining why growing of marijuana in one's greenhouse is not such a detail.[178]

The Court repeatedly stressed that the Fourth Amendment does not require the police to "shield their eyes when passing a home on public thoroughfares"[179] and treated the overflight as equivalent to the innocent passing of a home.[180] In a different approach, the California Court of Appeals obviously distinguished such a "focused" observation from the discovery during a routine patrol flight.[181]

In both cases, the Court did acknowledge that surveillance was taking place in an area that belonged to the curtilage of the suspect's home. For this reason, there was no doubt that an area in general protected by the Fourth Amendment was involved. Again, the purposeful and focused observation exclusively undertaken to uncover an activity the observed person was trying to shield from any scrutiny by a third party was equated by the Court with an occasional

---

[172] *Ibid.*

[173] The decision was delivered by White, who was joined by Scalia, Kennedy, and Rehnquist. O'Connor only joined in the judgment.

[174] *Ibid.* at 450.

[175] *Ibid.* at 451.

[176] *Ibid.* at 452. This is hardly a question to be judged under Fourth Amendment standards; see *ibid.* at 461–462 (Brennan, J., dissenting).

[177] *Ibid.* at 452.

[178] See *ibid.* at 463 (Brennan, J., dissenting) (warning that simply dismissing cases as drug cases imperils civil liberties). But see *Kyllo* v. *United States*, 533 U.S. 27, 37 (2001) (stating that in the home "all details are intimate details, because the entire area is held safe from prying government eyes").

[179] *Ciraolo*, 476 U.S. at 213.

[180] *Ibid.* at 213–214.

[181] *Ibid.* at 214 n.2.

observation by any member of the public. This approach does not take into consideration the difference between occasional observations by any member of the public and a focused observation within an ongoing criminal investigation, as outlined above.[182] The police, with considerable logistic input, were trying to uncover information about the activities at Riley's and Ciraolo's curtilage, both shielded against public scrutiny. Clearly, a collection of personal data took place here.

3.5. *Sense Enhancing Technologies*

Law enforcement officers for decades now do not exclusively rely on naked-eye observations. Sense enhancing technologies are being used to an increasing degree by the police. In *Kyllo* v. *United States*[183] the Court had to decide whether the use of a thermal imager by the police constitutes a search. The police suspected Kyllo of growing marijuana in his home. By measuring the amount of heat emanated from a house with a thermal imager it is possible to determine if high-intensity lamps frequently used for indoor marijuana growth may be in use. The police detected that some outer parts of Kyllo's home were relatively hot. Based on the thermal imaging and other information a warrant was issued and marijuana was found.[184] The Court held that an illegal search had taken place. Obviously more than naked-eye surveillance of a home had taken place. The question to be decided was "how much technological enhancement of ordinary perception" from a vantage point is "too much".[185] From a constitutional point of view the question is at what point the nature of a particular means of surveillance transforms such surveillance into a search in terms of the Fourth Amendment. In its ruling, the Court acknowledged that the realm of privacy protection has already shrunk with the use of modern surveillance technologies.[186] The Court emphasized that there is a "minimum", or "minimal" expectation of privacy that has to be protected or else police tech-

[182] See *supra* at III. 2.2.

[183] 533 U.S. 27 (2001).

[184] *Ibid.* at 29–30.

[185] *Ibid.* at 33.

[186] "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Ibid.* at 33–34.

nology would be allowed to erode privacy to a level no longer compatible with the Fourth Amendment.[187] This is equally true with regard to one's home because here "*all* details are intimate details".[188] According to the Court, the use of sense-enhancing technology goes beyond the constitutionally permissible if information is obtained that could otherwise not have been obtained without physical intrusion.

At the same time, the Court seems to limit this rule to such technologies that "are not in general public use".[189] To what extent the "public use" exception may lead to the acceptance of sense-enhancing technologies under constitutional requirements is not clear at all. The Court accepted certain sense-enhancing technologies in the past and there is no indication in *Kyllo* that the Court wants to deviate from these earlier decisions. Accordingly the use of searchlights[190] and flashlights[191] is admissible as long as the police officer made his or her observation from a vantage point where he or she had a right to be regardless of whether the observed person, object, or activity itself is situated in a space protected by the Fourth Amendment or not.[192] This is equally true with regard to the use of bifocals, field glasses or telescopes in order to magnify the object of a witness' vision.[193] However, whether the use of a highly sophisticated telescope would still be admissible after *Kyllo* seems to be questionable at least.[194]

The Court again seems to rely on the assumption that only such kind of governmental action constitutes an infringement that can be distinguished from observations by the general public. This seems to be flawed because there is little reason for a member of the public to carry out thermal imaging on a neighbor's home. Nevertheless, in case somebody is interested in using a thermal imager, for example,

---

[187] *Ibid.* at 34.

[188] *Ibid.* at 37 (emphasis in original).

[189] *Ibid.* at 34. The reasoning that such devices were not available to the general public seems to be arguable at least, see *ibid.* at 47 (Stevens, J., dissenting).

[190] *United States* v. *Lee*, 274 U.S. 559, 563 (1927).

[191] *Texas* v. *Brown*, 460 U.S. 730, 740 (1983).

[192] *United States* v. *Dunn*, 480 U.S. 294, 304–305 (1987).

[193] *United States* v. *Lee*, 274 U.S. 559, 563 (1927); *On Lee* v. *United States*, 343 U.S. 747, 754 (1952).

[194] Cf. *United States* v. *Kim*, 415 F.Supp. 1252 (1976) (use of an 800 millimeter telescope with a 60 millimeter opening from a distance of a quarter of a mile that allowed to observe which Journal suspect was reading).

because she or he wants to determine if his or her neighbor is wasting energy,[195] this would neither constitute nor result in immediate law enforcement action, as was the case in *Kyllo*.

The fact that Kyllo did use his home in a way that led to an emission of heat at least revealed data about the use of his apartment.[196] Since the police already knew that this apartment belonged to Kyllo,[197] they were trying to collect information about his habits. The police already had the suspicion that he was growing marijuana, they did not intend to look on his level of energy consumption for scientific purposes or anonymous research on energy consumption but the only purpose was to evaluate whether the heat emissions from his home could be an indication for the growth of marijuana. Consistently, since a high level of heat emissions from the house was detected the agent concluded that Kyllo was using halide lights to grow marijuana in his house.[198] From the collecting of data on his level of energy consumption information derived that lead to further investigative action. Consequently, it must be concluded that thermal imaging disclosed information about the personal or material circumstances of an identified individual.

3.6. *Electronic Tracking Devices/Beeper*

Electronic tracking devices like beepers are radio transmitters that emit periodic signals to be picked up by a radio receiver.[199] This allows police to follow the movements of a person at long distance without danger of being detected. In *Knotts* the Court compared surveillance by means of a beeper "principally to the following of an automobile on public streets and highways" which does not leave any reasonable expectation of privacy to the person observed.[200] The Court was convinced that the use of a beeper did not reveal other

[195] If wasting energy were a crime, the agency in charge would still have to follow up a tip by said neighbor. It would first have to collect its own data if such claim was true. If the neighbor delivered such data to the agency, no collection of data on behalf of the agency would have taken place. However, the agency at least would have to determine if the delivered data was reliable, thus *using* (instead of collecting) personal data before taking action against the person allegedly wasting energy.

[196] Cf. 533 U.S. at 49.

[197] *Ibid.* at 29.

[198] *Ibid.* at 30.

[199] *United States* v. *Knotts*, 460 U.S. 276, 277 (1983).

[200] *Ibid.* at 281.

facts than visual surveillance would have revealed.[201] In accordance with earlier rulings on the implications of the Fourth Amendment, the Court therefore was of the opinion that nothing "prohibited the police from augmenting the sensory facilities bestowed upon them at birth with such enhancements as science and technology afforded".[202] Since tracking devices are easily available to the general public[203] it seems to be fairly reasonable to conclude that *Kyllo* would not have any influence on that judgment.

In *Karo* the Court came to a different judgment than in *Knotts*. The suspects in this case carried to various places 10 cans of ether which could be used for the production of drugs. By visual surveillance and the use of a beeper, Drug Enforcement Administration agents were able to track the movement of said cans over a couple of months and finally applied for and obtained a search warrant for the house of one of the suspects, where cocaine and laboratory equipment were seized. By employing the beeper the Government was able to "obtain information that it could not have obtained by observation from outside the curtilage of the house".[204] Even though the Court deemed the use of a beeper "less intrusive than a full scale search", it revealed a "critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant".[205] Because information from inside the home was obtained without a warrant, the Court decided that an encroachment upon the Fourth Amendment's rights of the suspect had taken place.[206]

With regard to the pursuit of a car on public streets, a data protection approach would come to a different judgment. In *Knotts*,[207] police officers using a beeper were able to monitor the progress of different cars and their drivers carrying certain chemicals. The police believed these chemicals were supposed to be used in manufacturing illicit drugs. They also used the beeper signals to re-locate the chemicals after they lost these signals during visual observation of the car.

---

[201] Even though the police had lost the signal of the beeper for one hour (picking it up later with assistance of a helicopter based radio receiver) and had ended visual surveillance at this time, too. See *ibid.* at 278.

[202] *Ibid.* at 282.

[203] A full scale tracking device including software with maps of the whole US could be obtained early 2004 for less than 500 US$. See www.landairsea.com.

[204] *United States* v. *Karo*, 468 U.S. 705, 715 (1984).

[205] *Ibid.*

[206] *Ibid.* at 719.

[207] *United States* v. *Knotts*, 460 U.S. 276 (1983).

As a result, the police were collecting data about the movements of identified or identifiable individuals and information about certain items earlier purchased by these individuals. The observations lasted several days and ultimately lead to the officer's application for a search warrant.[208] For these reasons, it is without doubt that personal data about at least these two persons were collected during the surveillance.

In *Karo*,[209] the observation by use of a beeper (and other devices) revealed information about various movements of a huge amount of recently purchased ether to different private houses and commercial storages.[210] These movements were monitored because the law enforcement authorities suspected Karo of using the ether for the extraction of cocaine. The monitoring finally led to a private home where cocaine and laboratory equipment were seized and several persons were arrested. Some of the persons later indicted were those who earlier had moved the ether around to various locations and had been observed on these occasions. By use of the beeper, the law enforcement agents were able to collect data about their activities and involvement in the case.[211] Again, the beeper was used to collect data about natural persons and their involvement in an ongoing criminal conspiracy. As far as the reception of beeper signals is concerned, the inviolability of the home might take precedence over data protection principles if the case had to be judged under German law. Certainly, that would not lower the level of constitutional protection for the subject of surveillance, however. In contrast to the Supreme Court's privacy approach, even a denial of an encroachment upon the constitutional protection of the home would not result in a total lack of constitutional protection because the collection of personal data is obvious and data protection standards would apply.

3.7. *Wiretapping and Eavesdropping*

In *Katz*[212] the Court abandoned the physical trespass doctrine and ruled that the government's action of "electronically listening to and recording" the conversation of a person using a telephone booth "constituted a 'search and seizure' within the meaning of the Fourth Amendment".[213] This, however, applies to the "content" of

[208] *Ibid.* at 278–279.
[209] *United States* v. *Karo*, 468 U.S. 705 (1984).
[210] *Ibid.* at 708–710.
[211] See *ibid.* at 733–735, opinion of Stevens. J.
[212] 389 U.S. 347 (1967).
[213] *Ibid.* at 353.

communication only.[214] Similarly, eavesdropping aimed at (direct) oral communication (aural acquisition) may constitute a search within the meaning of the Fourth Amendment.[215] This has to be judged differently in cases where the person claiming privacy concerns has assumed the risk that the person she or he is talking to might be a traitor.[216]

Monitoring the contents of communication also constitutes a collection of personal data.[217] While the police are monitoring the contents of communication, the observed individuals as well as other participant(s) of such communication (third parties) are subject to scrutiny about their personal interactions, their thoughts and personal believings, their plans, personal, social, political, and other relations. As a result, eavesdropping may also result in the collection of data about one or more third parties at the same moment. Unlike the Supreme Court's approach,[218] even eavesdropping in a public place in general must be regarded as data collection, because it is not relevant that other's ears can hear what the person being observed is saying. Imagine somebody is using a loudspeaker to address a crowd.[219] The fact of addressing a crowd publicly as well as the content of the speech is information relating to an identified or identifiable individual. Therefore, even the observation of such activities results in data collection.

3.8. *Pen Register and Trap and Trace Devices*

The Supreme Court dealt with pen registers in two cases in the late 70s and Congress thereafter enacted legislation on the use of pen registers.[220] Different from wiretaps that intercept communication

[214] *United States* v. *N.Y. Tel. Co*., 434 U.S. 159, 166 (1977).

[215] *Berger* v. *New York*, 388 U.S. 41, 51 (1967).

[216] *United States* v. *White*, 401 U.S. 745, 752 (1971) (testimony of Government agent who secretly overheard the conversation of a suspect with an informant by means of a transmitter which an informant consented to wear during meetings is admissible in evidence).

[217] Under German law, art. 10 I Fed. Const. (*GG*) would be relevant, which protects the secrecy of telecommunications ("*Fernmeldegeheimnis*"). As a result, interception would rather be judged by (certainly not less) rigid standards of said constitutional provision.

[218] Cf. *United States* v. *White*, 401 U.S. 745, 747 (1971) (conversation in a restaurant).

[219] A possibly different judgment under the First Amendment is not relevant here.

[220] 18 U.S.C § 3121–3127.

and thus acquire the "contents" of communication, pen register devices do not catch sound. As outlined in *United States* v. *New York Telephone Co*.[221] pen registers only disclose "the telephone numbers that have been dialed".[222] According to the Court, these devices do not accomplish "aural acquisition" of communications nor is the identity of the caller or the recipient of the call recorded.[223] Two years later, in *Smith* v. *Maryland*[224] the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial".[225] This was justified with the fact that telephone users must convey the phone number of the person called to the telephone company to be able to complete a call. Moreover, according to the Court, "all subscribers realize" that the phone company "has facilities for making permanent records of the numbers they dial" for billing purposes. Besides, most people were thought to be aware of one common use of pen register devices: the identification of annoying or obscene callers.[226] Even though some people might have "subjective expectations" of privacy, in general telephone subscribers would not "harbour any general expectation that the numbers they dial will remain secret".[227] Even if they did so, society is not prepared to recognize such expectations as reasonable, according to the Court.[228] The Court stressed further that the telephone user also

[221] 434 U.S. 159.

[222] *Ibid.* at 167.

[223] *Ibid.* On the other hand, according to 18 U.S.C. § 3127(3) modern pen register devices may be able to acquire significantly more information than they used to in the late 70s, such as, for instance, bank account numbers and the Personal Identification Numbers (PIN) required to access such accounts. For technical details see, *e.g.*, Christian D. H. Schultz, Note, *Unrestricted Federal Agent: 'Carnivore' and the Need to Revise the Pen Register Statute*, 76 Notre Dame L. Rev. 1215 (2001). 18 U.S.C. § 3127(3) (West Supp. 2003), as amended, reads as follows: "[T]he term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . ."

[224] 442 U.S. 735 (1979).

[225] *Ibid.* at 742.

[226] *Ibid.* Conversely, it seems to be more practical in such cases to apply a trap and trace device to catch incoming calls, at least as long as no particular suspect has been identified.

[227] *Ibid.* at 743.

[228] *Ibid.*

"assumed the risk that the company would reveal to police the numbers he dialed".[229] Consequently, the use of pen registers by the police does not constitute an infringement of any right protected by the Fourth Amendment.

A trap and trace device captures incoming calls.[230] The Court has never explicitly decided on the admissibility of such devices under the Fourth Amendment. Nevertheless, in *United States* v. *New York Telephone Co*.[231] the Court held that pen register devices do not intercept because they do not acquire the contents of communication and therefore are not "posing a threat to privacy of the same dimension as the interception of oral communications".[232] Whether the Court's reasoning in *Smith* v. *Maryland*[233] does apply here equally seems to be questionable because telephone users certainly are aware that their telephone company is collecting information on their outgoing calls for billing purposes.[234] Contrary to this perception there seems to be little reason to assume that the public thinks incoming calls are registered also, because there is no necessity for technical or billing purposes.

From a data protection perspective there is no doubt that the phone number a person dials at his or her private phone or, for example, in a hotel room are personal data, because such number will divulge information about this person and his or her relations to the organization or natural person being called.[235] The fact that somebody calls a certain phone number, *e.g*., a union office, a political party, an organization that is engaged in the struggle for the legalization of drugs, or a clinic for the treatment of substances abuse, respectively, reveals information to the law enforcement agency monitoring these calls. The phone number dialed leads to the identification of the person or organization called and may lead to

[229] *Ibid*. at 744.

[230] 18 U.S.C.A. § 3127(4) (West Supp. 2003), as amended, reads as follows: "[D]evice or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . . shall not include the contents of any communication."

[231] 434 U.S. 159 (1977).

[232] *Ibid*. at 168.

[233] 442 U.S. 735 (1979).

[234] *Ibid*. at 742.

[235] But see note 217.

information about a person's contacts, beliefs, relationships and so forth.[236] For these reasons, telephone numbers are not at all without content.[237] This is even more obvious where the numbers dialed are part of the communication itself, for example, when accessing one's bank account via automated banking services.[238]

This classification is also applicable when it comes to trap and trace devices that collect data about incoming calls. Such data again may reveal information about personal, political, religious or other beliefs. Besides, data about the caller is being collected. That means not only the person under surveillance but that a third party is also the data subject.

3.9. *Examination of Bank and Utility Records*

In criminal investigations, police sometimes want to get access to information about bank records, or utility billing records,[239] and similar documents. In the case underlying the decision in *United States* v. *Miller*,[240] the Government issued a subpoena, which required two banks to produce "all records of accounts" of the suspect charged with various federal offenses.[241] The Court held that records of a bank are not "private papers" as protected by the Fourth Amendment.[242] Even the original checks and deposit slips were not considered confidential communications but negotiable instruments in commercial transactions because they were voluntarily conveyed to the bank and exposed to their employees. Accordingly, the "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government".[243] Interestingly the Court stated that the purpose of the Bank Secrecy

[236] See *Smith* v. *Maryland*, 442 U.S. at 748 (Stewart, J., dissenting).

[237] *Ibid.* at 751 (Marshall, J., dissenting).

[238] See, *e.g.*, *U.S. Telecom Ass'n* v. *FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000) (post-cut-through dialed digits can represent call content, *e.g.*, bank account numbers).

[239] See, *e.g.*, *Kyllo* v. *United States*, 533 U.S. 27, 30 (2001) (the use of such records was not contested in this case).

[240] 425 U.S. 435 (1976).

[241] *Ibid.* at 437–438.

[242] *Ibid.* at 440.

[243] *Ibid.* at 443 (with reference to *United States* v. *White*, 401 U.S. 754, 751–752 (1971). See also *United States* v. *Payner*, 447 U.S. 727, 732 (1980) (no privacy interest exists in bank records found in illegally seized briefcase).

Act was to facilitate law enforcement and not to protect the customers of the bank.[244] Even though the Supreme Court has never decided on using billing records of telephone companies or electric utilities there is little doubt that access to such information would be judged by the same standards.[245]

Again, from a data protection approach the outcome would be to the opposite. Financial data about a natural person, his or her wealth, data on financial contacts and transactions reveal highly sensitive information about "personal affairs, opinions, habits and associations," and the totality of one's bank records may provide a "virtual current biography".[246] For this reason, bank records provide data that contains personal information about the data subject, as long as a natural person is concerned. Even though utility bills may deliver less sensitive data, they still allow drawing conclusions upon one's living habits and patterns, as was the case in *Kyllo*,[247] for example. This is also true for methods of payment, because somebody under financial surveillance by the police may choose to pay in cash or try to find other ways to avoid surveillance. For these reasons, police in some criminal investigations use utility bills. It is therefore without doubt that utility bills contain personal data about the person(s) inhabiting the billed premises, such as high consumption of energy for the purpose of marijuana growing.

3.10. *Canine Sniff*

In *Place*,[248] the Court had to decide upon the seizure of a piece of luggage, the owner of which was suspected by DEA agents of carrying illicit drugs. Before entering the question of whether the seizure of such luggage for a period of 90 minutes was admissible[249] the Court questioned whether the investigative procedure itself that

---

[244] *United States* v. *Miller*, 425 U.S. 435, 444; see also *Cal. Bankers Ass'n* v. *Shultz*, 416 U.S. 21, 80–83 (1974) (Douglas, J., dissenting) (emphasizing this aim).

[245] RUDSTEIN ET AL., *supra* note 16, ¶ 2.03(2)(s) 16 (quoting many cases in favour of such an approach); LAFAVE, *supra* note 92, § 2.7(b) (referring to the "unfortunate decision" of the Court in *Miller*).

[246] *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (quoting *Burrows* v. *Superior Court*, 529 P.2d 590, 596 (Cal. 1974)); see also *Cal. Bankers Ass'n* v. *Shultz*, 416 U.S. 21, 78–79 (1974), (Powell, J., concurring) ("Financial transactions can reveal much about a person's activities, associations, and beliefs.")

[247] *Kyllo* v. *United States*, 533 U.S. 27, 30 (2001).

[248] *United States* v. *Place*, 462 U.S. 696 (1983).

[249] A question not relevant here.

led to the seizure was a search requiring probable cause. Since a "'canine sniff' by a well-trained narcotics detection dog" did not require opening the luggage and is thus "less intrusive than a typical search" this measure was not considered a search.[250] Besides such a sniff would only disclose the presence or absence of contraband items. Different from a "customary" search this information was regarded by the Court to be a limited disclosure that would spare the owner of the luggage the "embarrassment and inconvenience" of "more intrusive investigative methods".[251] For this reason, the whole procedure was regarded to be *sui generis* and not a search within the meaning of the Fourth Amendment because the searched object was located in a public space.[252]

The canine sniff is directed toward the detection of illicit drugs or other contraband. Whether a person is carrying such items is a matter of private choice, regardless of the legality of such behaviour. A narcotics detection dog sniffing clothing, body, or luggage of a person will smell scents that a human being may not be capable to smell. The use of such a dog is aimed to detect information that otherwise may not be obtained.[253] Nevertheless, the dog's actions and its reactions to what it smells cannot be regarded as the collection of data itself, because the dog obviously is not an agent of the government. Yet, the police are collecting information about the dog's behaviour with regard to an identified or identifiable person in a given case. This leads to information concerning the personal or material circumstances of an individual, because the police now have the information at hand that such person has a smell detected by a narcotics detection dog. In cases where the dog repeatedly pushes its nose and muzzle into the searched person's legs[254] the police officer will be aware of the dog's reaction and draw her or his conclusions from this fact. Such information (dog reacts in such-and-such way toward a certain person) is evaluated by the police and may lead to further action.

---

[250] *Place*, 462 U.S. at 707; but see *ibid.* at 720 (Brennan, J., concurring) (dog sniffs of people constitute a search).

[251] *Place*, 462 U.S. at 707.

[252] *Ibid.*

[253] See *Doe* v. *Renfrow*, 451 U.S. 1022, 1025 (1981) (Brennan, J., dissenting from denial of certiorari); Amanda S. Froh, *Rethinking Canine Sniffs: The Impact of Kyllo v. United States*, 26 SEATTLE U. L. REV. 337, 359 (2002) (a drug-sniffing canine provides data about the presence of drugs in a particular location).

[254] *Doe* v. *Renfrow*, 451 U.S. at 1023–1024 (dog repeatedly pushed its nose and muzzle into searched student's legs who was subsequently strip-searched).

Hence, the information obtained by a canine sniff, but not the canine sniff itself constitutes a collection of personal data.

IV. PROTECTION OF PERSONAL DATA – A LEGISLATIVE APPROACH

Perhaps Justice Scalia has a concept different from mine in mind when he notes that the privacy expectations that society is prepared to recognize as reasonable "unsurprisingly…bear an uncanny resemblance to those expectations of privacy" that the Court considers reasonable.[255] However, this hits the nail on the head. Perhaps most legal scholars will not dispute that the Supreme Court's two-pronged privacy test is flawed in itself and does not provide sufficient protection of legitimate interests of the individual in cases of police surveillance. This is especially true when the Court excludes a certain surveillance technique by simply denying the use of such technique as being a search at all. Having this in mind, the lack of legislative action and limitations on police activities is well described as a "vacuum of subconstitutional controls upon police practices".[256]

One commentator has stated that the courts are best suited to deal with upcoming legal problems when it comes to new computer technologies because incremental judicial response is "often superior to instant legislative solutions of global nature".[257] One might think this is true for new computer technologies due to their fast technological developments and changes. Given the rapid changes in some technologies, legislation seems to run the risk of becoming obsolete rather quickly.[258] A possible response to such changes might be getting used to a rather abstract type of regulations instead of the sometime meticulous regulation of every tiny detail and eventuality in American law. However, judicial control alone is not an appropriate tool with regard to Fourth Amendment privacy, as the Supreme Court has demonstrated for decades now. First, only some measures of police surveillance techniques rely on new technologies while many others use longstanding practices, as demonstrated above. Second,

[255] *Minnesota* v. *Carter*, 525 U.S. 83, 97 (Scalia, J., concurring).

[256] Amsterdam, *supra* note 25, at 380.

[257] Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 311 (2002).

[258] *Ibid.* at 312.

the "common law process" of judge-made law and judicial interpretation of existing statutes[259] favored for rapidly developing new technologies resulted in neither clear-cut rules when it comes to Fourth Amendment privacy nor sufficient protection against governmental surveillance.

It is probably a common understanding among most legal scholars that a large part of police activities are not specifically authorized by the law but simply conducted in discharge of police duties.[260] For this reason, some want to limit police *discretion*[261] to conduct searches and seizures by either legislation, or by administrative police-made rules and regulations, subject to judicial review of their reasonableness.[262] Most police departments today have a very comprehensive set of administrative rules. Police-made rules, though, from my point of view, are not sufficient to determine intrusions upon civil liberties. Police rulemaking creates the potential for abuse[263] because it lacks sufficient control by the people. The executive branch of government does not make the law, but only has to execute the powers vested in it by the Constitution, or a statute.[264]

Prior judicial approval is not a valid remedy either. In case of police surveillance, "judicial approval prior to initiation of a search

[259] Sherry, *supra* note 257, at 317.

[260] Amsterdam, *supra* note 25, at 386. See also Ku, *supra* note 25, at 1328 (in many instances police are not bound by any legal or constitutional restraints when it comes to surveillance and, especially, application of new technologies); Mark J. Young, Note, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1088 (2001) (in substance, the Fourth Amendment gives law enforcement "virtually unlimited power" of surveillance unless the public and the courts become aware).

[261] See, *e.g.*, Wayne R. LaFave, *Controlling Discretion by Administrative Regulations: The Use, Misuse, and Nonuse of Police Rules and Policies in Fourth Amendment Adjudication*, 89 MICH. L. REV. 442, 447–451 (1990). LaFave's basic assumption that there is a need for guidelines by police agencies shall not be disputed in general. My proposal is not directed at limiting discretion but I suggest to 're-invent' the very basis of police surveillance.

[262] Amsterdam, *supra* note 25, at 409; Young, *supra* note 261, at 1095–1098 (legislative or administrative rulemaking could serve as a prerequisite for electronic surveillance); see also ABA Standards for Criminal Justice: Electronic Surveillance, 3rd ed., Section B: Technologically-Assisted Physical Surveillance, Standard 2-9.1.(b) and (e) (stating that there may be a need of legislative or administrative rulemaking for technologically assisted physical surveillance due to its possible impact on privacy, freedom of speech, association, and the openness of society).

[263] Young, *supra* note 260, at 1097–1098.

[264] See *Youngston Sheet & Tube Co.* v. *Sawyer*, 343 U.S. 579, 587–589 (1952).

or surveillance''[265] today rather is the exception than the rule, due to the Court's various exceptions for exigent circumstances and other warrantless searches.[266] Since prior judicial review in reality no longer is a valid counterbalance for police conduct, police-made (administrative) rules alone can no longer constitute a sufficient safeguard of Fourth Amendment liberties. Administrative rulemaking certainly does not provide the appropriate means for such a radical shift in protection against police surveillance.

Some scholars give preference to legislative activity with regard to police surveillance. They claim that legislatures are ''institutionally more competent than courts to make the types of policy decisions associated with authorizing government surveillance''.[267] Even the Supreme Court or at least some of the Justices sometimes seem to feel a need for statutory definitions when it comes to Fourth Amendment cases.[268] Supposed they were not more competent, legislators are at least politically accountable. Legislation would even force them to take over accountability for certain techniques of police surveillance. For this reason, they may be willing to evaluate the policy implications of certain surveillance technologies and balance the threats to privacy and the potentials for abuse against the interests of law enforcement. ''Whatever one might think of the legislative process, it is more likely to take the interests of the general public into account . . . than courts who are asked to make such decisions in cases in which a search revealed evidence . . . and the only remedy is the exclusion of that evidence.''[269] Relying on the Supreme Court's long-standing rule that privacy expectations are reasonable if society is prepared to accept them it is suggested that society itself should

[265] *United States* v. *United States District Court*, 407 U.S. 297, 321 (1972).

[266] See, *e.g.*, Bloom, *Warrant Requirement – The Burger Court Approach*, 53 U. COLO. L . REV. 691, 744 (1982) (''the Court's preference is in words, not in deeds''); Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 882 (1991) (''in practice warrants are the exception rather than the rule'').

[267] Ku, *supra* note 25, at 1375.

[268] See John Q. Barrett, *Deciding the Stop and Frisk Cases: A Look Inside the Supreme Court's Conference*, 72 ST. JOHN'S L. REV. 749, 816 (1998) (citing then Chief Justice Warren who wanted the Court ''to try to write our own annotated stop and frisk statute'').

[269] Ku, *supra* note 25, at 1375.

define what is reasonable and what is not.[270] Thus, expansion of the objects of privacy protection becomes possible by the ''good judgment . . . of the people through their representatives in the legislature''.[271] When the use of a specific technology becomes ''so ubiquitous that the public as a whole appreciates its threats'',[272] society might want to rely upon the legislature. To the contrary, as long as the public does not consider a technology to be a threat, legislation may be far away. ''[R]equiring the use of surveillance technologies to be authorized by statute recognizes that the people should determine just how much power government should wield.''[273] This would lead back to what is perhaps the basic idea behind the Fourth Amendment, that the people should control the power of Government. As one commentator put it, ''the people themselves must decide just what is reasonable search and seizure''.[274] As is the case with Title III the ''courts will not initially decide for society what society wants to do''.[275] Instead, society will decide on that question first. That does not amount to the abandonment of judicial control but the courts will have to determine if surveillance in a given case is admissible under statutory law. Constitutional limitations on such legislation obviously also apply.[276] From my point of view, Professor Amsterdam's pessimistic assumption that control of the police for lawmakers is a ''politically suicidal undertaking''[277] alone cannot be a sufficient hindrance to propose such an undertaking.

---

[270] Rich Haglund, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?*, 5 VAND. J. ENT. L & PRAC. 137, 146 (2003) (when expectations change society can pass legislation that reflects those changes).

[271] *Minnesota* v. *Carter*, 525 U.S. 83, 97–98 (Scalia, J., concurring).

[272] See Ku, *supra* note 25, at 1370.

[273] *Ibid.* at 1375.

[274] Gerard V. Bradley, *The Constitutional Theory of the Fourth Amendment*, 38 DE PAUL L. REV. 817, 870 (1989) (proposing to ''deactivate'' the reasonable clause, *ibid.* at 871).

[275] *Ibid.* at 870.

[276] *Ibid.* at 871 (statute that authorizes, *e.g.*, stopping only blacks could not pass equal protection muster).

[277] Amsterdam, *supra* note 25, 378–379 (stating that legislators in the past never did and are not likely in the future to protect persons under investigation by the police). For this reason, perhaps, Amsterdam proposes substantive rulemaking. *Ibid.* at 417–428.

The common law provides that the "eye cannot by the laws of England be guilty of a trespass".[278] Visual observation of what a person knowingly exposes to the public is no search at all, according to the Supreme Court.[279] While the Fourth Amendment may not set other limits to police surveillance in public, a statute may well do so. The legislator could establish a right of data protection with regard to police surveillance. Such legislation might not only expand Fourth Amendment privacy protection but might go beyond Fourth Amendment protections,[280] as is the case with Title III[281] for instance. Today, police surveillance resulting in the collection of information about a person falling outside (traditional) Fourth Amendment protection in general is not subject to judicial control at all.[282] This is only different in the rare case where other constitutional provisions or statutory provisions are concerned. In consequence, data protection would no be part of Fourth Amendment protection but something that goes beyond the limitations of this constitutional provision. Every citizen should be protected against police surveillance that results in the collection, storage, processing, or use of personal data except such when activity is warranted by a specific statutory provision.[283]

The major advantage of such an approach when compared with current privacy protection is that every citizen and the police could learn from a given statute what legitimate police surveillance is and what is not. Obviously, there will be different understandings and uncertainties in interpreting a given statute. Resolving these problems would be the important task of the courts. In spite of this, the courts no longer would have to rely on the cryptic idea of reasonable expectations of privacy that society (*i.e.*, judges) are prepared to accept as reasonable, which will be construed by a court perhaps several years later. Instead, everyone is able to get a fair idea whether a certain surveillance technique is provided for in the statute or not. If this is not the case, its application is illegal regardless what society or

[278] *Boyd* v. *United States*, 116 U.S. 616, 628 (1886).

[279] *Kyllo* v. *United States*, 533 U.S. 27, 32 (2001).

[280] Cf. *Brown* v. *Waddell*, 50 F.3d 285, 290 (4th Cir. 1995) (Title III requirements in many cases exceed constitutional search warrant requirements).

[281] 18 U.S.C.A. §§ 2510–2520 (West 2003).

[282] Katz, *supra* note 51, at 553; see also Amsterdam, *supra* note 25, at 356 (what is not a search is not required to be reasonable under Fourth Amendment standards).

[283] Cf. Solove, *supra* note 35, at 1085 (referring to data collection by government in general).

a court deem reasonable in hindsight. This approach is not as revolutionary as it might seem at first glance, but a well-known legislative technique applied, *e.g.*, in the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[284] Title III might be a good starting point as a concept of statutory regulation when it comes to the protection of citizens against collection, storage, processing, and use of their personal data by means of police surveillance. Since such legislation goes beyond Fourth Amendment protection, an exclusionary remedy comparable to Title III[285] may be necessary because evidence obtained in violation of the statute may otherwise be admissible in the courts.[286] In addition, the Supreme Court may adopt a rule that data collection etc. by the police is *per se* unreasonable unless the legislative branch has established rules governing such activities by the police.[287]

With regard to the proliferation of communication technologies that are major methods of police surveillance (*e.g.* wiretapping, pen registers, surveillance of email and Internet use etc.), some commentators stress that these technologies pose great challenges to the competing interest of privacy on the one hand and law enforcement on the other hand.[288] This is not only true from a privacy perspective but also when it comes to the protection of personal data. Thus, a comprehensive approach should address these technologies as well.

For sure, this approach does not imply or require absolute protection of any personal data against police surveillance because this would run against the general interest of law enforcement. A legislative approach does not constrict the lawful use of surveillance techniques *in toto*. Accordingly, protection has to be balanced with the competing interests of law enforcement to a certain extent. Supposed there is some legitimate need on the part of the government, it has to be determined whether this interest outweighs the individual's

---

[284] 18 U.S.C.A. §§ 2510–2520 (West 2003). Title III might be a good example that Congress is able to regulate the matter, see CRAGI M. BRADLEY, THE FAILURE OF THE CRIMINAL PROCEDURE REVOLUTION 148 (1993).

[285] See 18 U.S.C. § 2515 (2000).

[286] Cf. Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance*, 86 MINN. L. Rev. 1393, 1436 (2002) (proposing a statute on visual surveillance comparable to Title III).

[287] Cf. Young, supra note 260, at 1095.

[288] See, *e.g.*, Elmore, *supra* note 32, at 1080–1083; Kimberly A. Horn, *Privacy versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 FORDHAM URB. L. J. 2233, 2271–272 (2002) (both with reference to Carnivore, a system to intercept and collect electronic communications).

interest in protecting his or her personal data.[289] As is the case with other statutory provisions, balancing liberty interests with the government's law enforcement interest has to take place on the statutory level itself. It should not be left to the police under a general reasonable standard, but the legislator has to set the course. As outlined earlier, the balancing should be left to the "good judgment... of the people through their representatives in the legislature".[290] This obviously does not cut off the possibility of judicial review in every single case.

Whether Congress, or the States under their broad police power should implement such laws has to be determined in the light of the limitations on Congress' legislative powers on one hand and the exact content of such a piece of legislation on the other hand.[291]

V. CONCLUSION

The demise of Fourth Amendment privacy seems to be inevitable, at least as far as other places than the innermost sanctuaries of the private home are concerned. Who does not take refuge in his home in general has no reliable expectation of privacy. This results from the Supreme Court's doctrine that it is only such expectations of privacy that are constitutionally protected that the Court is prepared to recognize as reasonable. These are very few. Resurrection seems not to be within the bounds of probability. To moan about better times in Fourth Amendment cases does not offer relief. Instead, it seems necessary to look for a different approach.

As far as police surveillance is concerned, an approach that aims at the protection of personal data might be a valuable substitute. This would result in a dramatic shift of perspective. What a (natural) person knowingly exposes to the public would no longer be the borderline when it has to be decided whether an intrusion has taken

[289] Cf. Stuntz, *supra* note 51, at 1031 (proposing the balancing of privacy interest with the governmental interest of gaining information in a given case).

[290] *Minnesota* v. *Carter*, 525 U.S. 83, 97–98 (Scalia, J., concurring).

[291] See, *e.g.*, *United States* v. *Lopez*, 514 U.S. 549, 567 (1995) (congressional Commerce Clause cannot be converted into general police power held only by the states). Others do not doubt that Congress has legislative power to enact a broad statute on criminal procedure, see, *e.g.*, BRADLEY, *supra* note 284, at 145 (proposing a special commission with continuing existence that makes proposals for Congress that would be limited to voting on such proposals); see also *supra* note 262 (all authors proposing either legislative action or administrative rulemaking).

place or not. Personal data is any information concerning the personal or material circumstances relating to an identified or identifiable individual. Thus, an intrusion takes place whenever the police look for information about a person. This is the case when the police are looking for specific information or data, or target a specific location, person, or object. Even though every other person might be able to do so as well, it constitutes an intrusion if such activity is carried out by the police. The basic rationale behind this approach is that the police have vast resources of data collection and data storing at their disposal and may use such data for future law enforcement activities against the observed person. Besides, the police have the constitutional power to deprive the person under surveillance of his or her freedom. This clearly distinguishes the police from every citizen and therefore the government and its agents cannot be treated like a citizen when it comes to information gathering.

Since Fourth Amendment privacy protection is in vain, either police regulations (administrative rulemaking) or statutory provisions should rule collection, storage, use, and transfer of personal data by the police. From my point of view, legislative action seems to be preferable. The executive branch of government cannot make the law. The police only have to execute the powers vested in it by the Constitution, or a statute. By legislative action, the people regain control over the government instead of being a subject of control under the nowadays virtually unlimited discretion of police officers. Besides, legislative rules themselves as well as the application of such rules in every single case are subject to judicial control.